The NP-Completeness of Reflected Fragments of Justification Logics

Samuel R. Buss[1,⋆] and Roman Kuznets[2,⋆⋆]

[1] Department of Mathematics, University of California, San Diego
La Jolla, CA 92093-0112, USA
sbuss@ucsd.edu
[2] Institut für Informatik und angewandte Mathematik, Universität Bern
Neubrückstrasse 10, CH-3012 Bern, Switzerland
kuznets@iam.unibe.ch

Abstract. Justification Logic studies epistemic and provability phenomena by introducing justifications/proofs into the language in the form of justification terms. Pure justification logics serve as counterparts of traditional modal epistemic logics, and hybrid logics combine epistemic modalities with justification terms. The computational complexity of pure justification logics is typically lower than that of the corresponding modal logics. Moreover, the so-called reflected fragments, which still contain complete information about the respective justification logics, are known to be in NP for a wide range of justification logics, pure and hybrid alike. This paper shows that, under reasonable additional restrictions, these reflected fragments are NP-complete, thereby proving a matching lower bound.

1 Introduction and Main Definitions

Justification Logic is an emerging field that studies provability, knowledge, and belief via explicit proofs or justifications that are part of the language. A justification logic is essentially a refined analogue of a modal epistemic logic. Whereas a modal epistemic logic uses the formula $\Box F$ to indicate that F is known to be true, a justification logic uses $t : F$ instead, where t is a term that describes a 'justification' or proof of F. This construction allows justification logics to reason about both formulas and proofs at the same time, avoiding the need to treat provability at the metalevel.

Because Justification Logic can reason directly about explicit proofs, it provides more concrete and constructive analogues of modal epistemic logics. For example, the modal distribution axiom $\Box(F \to G) \to (\Box F \to \Box G)$ is replaced in

⋆ Partially supported by NSF grant DMS–0700533.
⋆⋆ Supported by Swiss National Science Foundation grant 200021–117699. The initial stages of the research were partially supported by a CUNY Graduate Center Research Grant for Doctoral Students.

Justification Logic by the axiom $s{:}(F \to G) \to (t{:}F \to (s \cdot t){:}G)$. The latter replaces the distribution axiom with a computationally explicit construction. Justification logics are very promising for structural proof theory and have already proven to be fruitful in finding new approaches to common knowledge ([Art06]) and Logical Omniscience Problem ([AK06]). For further discussion on the various applications of Justification Logic, see [Art08b].

The goal of the present paper is to prove the NP-hardness of the Derivability Problem for the reflected fragments of justification logics, matching the already known upper bound. We begin by reviewing some definitions of justification logics.

The first justification logic, the Logic of Proofs LP, was introduced by Artemov [Art95] to provide a provability semantics for the modal logic $\mathsf{S4}$ (see also [Art01]). The language of LP

$$F ::= p \mid \bot \mid (F \to F) \mid t{:}F \ ,$$
$$t ::= x \mid c \mid (t \cdot t) \mid (t + t) \mid !\, t$$

contains an additional operator $t{:}F$, read 'term t serves as a justification/proof of formula F.' Here p stands for a sentence letter, x for a justification variable, and c for a justification constant.

Statements $t{:}F$ can be seen as refinements of modal statements $\Box F$ because the latter say that F is known whereas the former additionally provide a rationale for such knowledge. This relationship is demonstrated through the recursively defined operation of *forgetful projection* that maps justification formulas to modal formulas: $(t{:}F)^\circ = \Box(F^\circ)$, and commutes with Boolean connectives: $(F \to G)^\circ = F^\circ \to G^\circ$, where $p^\circ = p$ and $\bot^\circ = \bot$.

Axioms and rules of LP:

A1. A complete axiomatization of classical propositional logic by finitely many axiom schemes; rule *modus ponens*

A2. *Application Axiom* $s{:}(F \to G) \to (t{:}F \to (s \cdot t){:}G)$

A3. *Monotonicity Axiom* $s{:}F \to (s + t){:}F, \quad t{:}F \to (s + t){:}F$

A4. *Factivity Axiom* $t{:}F \to F$

A5. *Positive Introspection Axiom* $t{:}F \to !\, t{:}t{:}F$

R4. *Axiom Internalization Rule*: $\dfrac{}{c{:}A}$

where A is an axiom and c is a justification constant

LP is the exact counterpart of $\mathsf{S4}$ (note the similarity of their axioms): namely, let $X^\circ = \{F^\circ \mid F \in X\}$ for a set X of justification formulas and let LP be identified with the set of its theorems, then

Theorem 1 (Realization Theorem, [Art95, Art01]). $\mathsf{LP}^\circ = \mathsf{S4}$.

For some applications (e.g., to avoid Logical Omniscience [AK06] or to study self-referentiality [Kuz08c]) the use of constants needs to be restricted; this is achieved using *constant specifications*. A *constant specification* $\mathcal{CS}$ is a set of instances of rule R4:

$$\mathcal{CS} \subseteq \{c{:}A \mid A \text{ is an axiom, } c \text{ is a justification constant}\} \ .$$

Given a constant specification $\mathcal{CS}$, the logic $\mathsf{LP}_{\mathcal{CS}}$ is the result of replacing R4 in LP by its relativized version:

$\mathrm{R4}_{\mathcal{CS}}$. *Relativized Axiom Internalization Rule*: $\dfrac{c{:}A \in \mathcal{CS}}{c{:}A}$

For the Realization Theorem to hold, i.e., for $(\mathsf{LP}_{\mathcal{CS}})^{\circ} = \mathsf{S4}$, it is necessary and sufficient that $\mathcal{CS}$ be *axiomatically appropriate*:

Definition. A constant specification $\mathcal{CS}$ is called:

- *axiomatically appropriate*[3] if every axiom is justified by at least one constant;
- *schematic*[4] if each constant justifies several (maybe 0) axiom schemes and only them;
- *schematically injective*[5] if it is schematic and each constant justifies no more than one axiom scheme.

Whereas it is well known that the Derivability Problem for $\mathsf{S4}$ is PSPACE-complete ([Lad77]), it was shown in [Kuz00] that the same problem for $\mathsf{LP}_{\mathcal{CS}}$ is in Π_2^p for any schematic $\mathcal{CS}$ (we always assume $\mathcal{CS}$ to be polynomial time decidable); in particular, LP itself is in Π_2^p. Milnikel in [Mil07] proved a matching lower bound, the Π_2^p-hardness of $\mathsf{LP}_{\mathcal{CS}}$ under the assumption that $\mathcal{CS}$ is axiomatically appropriate and schematically injective.

The so-called *reflected fragment* rLP of the Logic of Proofs was first studied by N. Krupski in [Kru03] (see also [Kru06]):

Definition. For any justification logic $\mathsf{JL}_{\mathcal{CS}}$ with a constant specification $\mathcal{CS}$, its reflected fragment is

$$\mathsf{rJL}_{\mathcal{CS}} = \{t{:}F \mid \mathsf{JL}_{\mathcal{CS}} \vdash t{:}F\} \ .$$

We will write $\mathsf{rJL}_{\mathcal{CS}} \vdash t{:}F$ to mean $t{:}F \in \mathsf{rJL}_{\mathcal{CS}}$.

The reflected fragment bears complete information about the logic as the following theorem shows:

Theorem 2 ([Kru03, Kru06]). *For any axiomatically appropriate $\mathcal{CS}$,*

$$\mathsf{LP}_{\mathcal{CS}} \vdash F \qquad \Longleftrightarrow \qquad (\exists t)\mathsf{rLP}_{\mathcal{CS}} \vdash t{:}F \ .$$

The $\Longrightarrow$-direction constitutes the Constructive Necessitation Property (for details, see [Art01]); the $\Longleftarrow$-direction easily follows from Factivity Axiom A4.

Theorem 3 ([Kru03, Kru06]). *For any schematic $\mathcal{CS}$, the Derivability Problem for $\mathsf{rLP}_{\mathcal{CS}}$ is in NP.*

[3] The term is due to Fitting.
[4] The term is due to Milnikel although the idea goes back to Mkrtychev.
[5] The term is due to Milnikel.

To prove this theorem, N. Krupski developed an independent axiomatization for $\mathsf{rLP}_{\mathcal{CS}}$ that we will call the $*$-calculus.

Axioms and rules of the $*$-calculus:

$*\mathcal{CS}$. For any $c{:}A \in \mathcal{CS}$ $\qquad$ axiom $c{:}A$

$*$A2. *Application Rule* $\qquad \dfrac{s{:}(F \to G) \qquad t{:}F}{s \cdot t{:}G}$

$*$A3. *Sum Rule* $\qquad \dfrac{s{:}F}{s+t{:}F} \qquad \dfrac{t{:}F}{s+t{:}F}$

$*$A5. *Positive Introspection Rule* $\qquad \dfrac{t{:}F}{!t{:}t{:}F}$

In this paper, we prove the matching lower bound for $\mathsf{rLP}_{\mathcal{CS}}$, namely that the Derivability Problem for $\mathsf{rLP}_{\mathcal{CS}}$ is NP-complete. The proof is by a many-one polynomial-time reduction from a known NP-complete problem, the Vertex Cover problem. As in Milnikel's lower bound for $\mathsf{LP}_{\mathcal{CS}}$, we have to impose the additional restriction that $\mathcal{CS}$ is axiomatically appropriate and schematically injective.

The paper is structured as follows. Section 2 defines a coding of a graph by propositional formulas and shows how the existence of a vertex cover can be described in terms of these formulas. Section 3 develops justification terms that encode several standard methods of propositional reasoning. Although the formulas that describe the existence of a vertex cover depend on the cover itself rather than only on its size, Sect. 4 shows how to eliminate this dependency by using the terms from Sect. 3 to encode particular derivations of the formulas from Sect. 2. Section 5 finishes the proof of the polynomial-time reduction. Section 6 discusses extending this result to other justification logics.

2 Graph Coding and Preliminaries

A graph $G = \langle V, E\rangle$ has a finite set V of vertices and a finite set E of undirected edges. We assume w.l.o.g. that $V = \{1, \ldots, N\}$ for some N, and we represent an edge e between vertices k and l as the set $e = \{k, l\}$ with the endpoints denoted by $v_1(e) < v_2(e)$. A vertex cover for G is a set C of vertices such that each edge $e \in E$ has at least one endpoint in C. The Vertex Cover problem is the problem of, given a graph G and an $L \geq 0$, determining if G has a vertex cover of size $\leq L$. The Vertex Cover problem is one of the classic NP-complete problems.

We define below formulas F_V, F_C, and F_G that will help build a many-one reduction from Vertex Cover to $\mathsf{rLP}_{\mathcal{CS}}$. These formulas will include large conjunctions. To avoid the dependence of the $\mathsf{LP}_{\mathcal{CS}}$-derivations on the vertex cover, we will use balanced conjunctions (see [BB93]):

Definition. Each formula is a *balanced conjunction of depth* 0. If A and B are both balanced conjunctions of depth k, then $A \wedge B$ is a *balanced conjunction of depth* $k+1$.

Clearly, a balanced conjunction of depth k is also a balanced conjunction of depth l for any $0 \leq l \leq k$. Thus, we are mainly interested in how deeply a given formula is conjunctively balanced. For any conjunction $C_1 \wedge \cdots \wedge C_{2^k}$ of 2^k formulas, we assume that the omitted parentheses are such that the resulting balanced conjunction has the maximal possible depth, i.e., depth $\geq k$.

We also need to refer to C_i's that form $F = C_1 \wedge \cdots \wedge C_{2^k}$. The following inductive definition of *depth k conjuncts*, or simply *k-conjuncts*, generalizes the definition of *conjuncts* in an ordinary conjunction:

Definition. Each formula is a 0-*conjunct* of itself. If $C \wedge D$ is a k-conjunct of formula F, then C and D are both $(k+1)$-*conjuncts* of F.

For instance, the conjuncts of an ordinary conjunction are its 1-conjuncts; all C_i's in $C_1 \wedge \cdots \wedge C_{2^k}$ are its k-conjuncts. More generally, any balanced conjunction of depth k must have exactly 2^k occurrences of k-conjuncts (with possibly several occurrences of the same formula).

To make full use of balanced conjunctions, it is convenient to restrict attention to instances of the Vertex Cover problem for graphs in which both the number of vertices and the number of edges are powers of 2. These are called *binary exponential graphs*. It is also helpful to only consider vertex covers whose size is a power of 2; these we call *binary exponential* vertex covers. Fortunately, the version of the Vertex Cover (VC) problem restricted to binary exponential graphs and their binary exponential vertex covers is also NP-complete:

Theorem 4. *The Binary Vertex Cover (BVC) problem of determining for a given binary exponential graph G and a given $l \geq 0$ whether G has a vertex cover of size $\leq 2^l$ is NP-complete.*

Proof. Since BVC is an instance of the standard VC problem, and since VC is NP-complete, it suffices to construct a polynomial-time many-one reduction from VC to BVC. Suppose we are given an instance of VC; namely, we are given a graph G_0 and an integer L and wish to determine if G_0 has a vertex cover of size $\leq L$. We give a polynomial time procedure that constructs a binary exponential graph G and a value l so that G_0 has a vertex cover of size $\leq L$ iff G has a vertex cover of size $\leq 2^l$. The graph G is constructed in three stages; each stage causes only a constant factor increase in the size of the graph.

Stage 1. Increasing the size of the vertex cover. Let $0 \leq L' < L$ such that $L + L' = 2^l - 1$ for some integer $l \geq 0$. The graph $G' = \langle V', E' \rangle$ is obtained from G_0 by adding $2L'$ new vertices broken into L' disjoint pairs with the vertices in each pair joined by a new edge (L' new edges overall). G_0 has a vertex cover of size $\leq L$ iff G' has a vertex cover of size $\leq 2^l - 1$.

Stage 2. Increasing the number of edges. Choose integer $0 < M'' \leq |E'|$ such that $|E'| + M'' = 2^m$ for some integer $m \geq 0$. The graph $G'' = \langle V'', E'' \rangle$ is obtained by adding $M'' + 1$ new vertices to G' with one of these vertices joined to all M'' others (M'' new edges overall). G' has a vertex cover of size $\leq 2^l - 1$ iff G'' has a vertex cover of size $\leq 2^l$.

Stage 3. Increasing the number of vertices. Choose integer $0 \leq N''' < |V''|$ such that $|V''| + N''' = 2^n$ for some integer $n \geq 0$. The graph $G = G'''$ is obtained by adding N''' isolated vertices to G''. G'' has a vertex cover of size $\leq 2^l$ iff G''' has a vertex cover of size $\leq 2^l$.

It is clear from the construction that G is a binary exponential graph such that G_0 has a vertex cover of size $\leq L$ iff G has a vertex cover of size $\leq 2^l$. $\square$

Definition. Let $G = \langle V, E\rangle$ be a binary exponential graph with edge set $E = \{e_1, \ldots, e_{2^m}\}$. Let $C = \{i_1, i_2, \ldots, i_{2^l}\} \subseteq V$ be a possible binary exponential vertex cover for G, where $i_1 < i_2 < \cdots < i_{2^l}$. We define the following formulas:

a. $F_C = p_{i_1} \wedge \cdots \wedge p_{i_{2^l}}$.
b. For each edge $e = \{k, l\}$, where $k < l$, $F_e = p_k \vee p_l = p_{v_1(e)} \vee p_{v_2(e)}$.
c. $F_G = F_{e_1} \wedge \cdots \wedge F_{e_{2^m}}$.

The proof of the following properties of the translation is an easy exercise ($\vdash$ denotes derivability in classical propositional logic):

Lemma 5. *For any binary exponential graph $G = \langle V, E\rangle$ and any binary exponential set $C \subseteq V$,*
1. $\vdash F_V \rightarrow F_G$;
2. $\vdash F_V \rightarrow F_C$;
3. $\vdash F_C \rightarrow F_G$ *iff* *C is a vertex cover for G.*

Our goal is to reduce BVC to derivability in $\mathsf{rLP}_{\mathcal{CS}}$ for a certain class of $\mathcal{CS}$. To this end, we take a particular derivation of $F_V \rightarrow F_G$ that proceeds by first proving $F_V \rightarrow F_C$, followed by an attempt at a proof of $F_C \rightarrow F_G$ that succeeds iff C is a vertex cover. Finally, hypothetical syllogism (HS) is applied to infer $F_V \rightarrow F_G$. We further encode this derivation as a justification term t so that $\mathsf{rLP}_{\mathcal{CS}} \vdash t : (F_V \rightarrow F_G)$ iff C is a vertex cover. In BVC we need to determine whether there exists a vertex cover of (at most) a given size rather than whether a given set of vertices is a vertex cover. Thus, $t{:}(F_V \rightarrow F_G)$ should not depend on C but may (and should) depend on the size of C. Since C has already been "syllogized away" from formula $F_V \rightarrow F_G$, it remains to make sure that term t only depends on the size of C. Although the derivations of $F_V \rightarrow F_C$ and $F_C \rightarrow F_G$ have C explicitly present in them, the terms encoding them, and therefore t, can be made independent of C. This is the main reason why we use balanced conjunctions: this way all k-conjuncts are interchangeable.

Note about the use of constants. Throughout the paper, the minimum requirement on $\mathcal{CS}$ would be axiomatic appropriateness and schematicness. As a consequence, we can always assume that for any axiom scheme there exists a constant justifying it. So it makes sense to choose one such constant for each axiom scheme. The list of names for these fixed constants along with the corresponding

axiom schemes consistently used in the paper can be found below:

$$\begin{array}{lll}
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_1 & : \ (X \to (Y \to X)) \\
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_2 & : \ ((X \to (Y \to Z)) \to ((X \to Y) \to (X \to Z))) \\
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_{\wedge 1} & : \ (X \wedge Y \to X) \\
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_{\wedge 2} & : \ (X \wedge Y \to Y) \\
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_{\wedge} & : \ (X \to (Y \to X \wedge Y)) \\
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_{\vee 1} & : \ (X \to X \vee Y) \\
\mathsf{rLP}_{\mathcal{CS}} \vdash & c_{\vee 2} & : \ (Y \to X \vee Y)
\end{array}$$

Note that we have assumed that certain axiom schemes are present among the propositional axioms chosen for A1. The beginning of Sect. 5 discusses why this assumption is not essential.

3 Justification Terms Encoding Propositional Reasoning

For all lemmas in the section, schematicness and axiomatic appropriateness are sufficient for the $\Longleftarrow$-direction; schematic injectivity is required for the $\Longrightarrow$-direction only.

The size of terms is defined in a standard way: $|c| = |x| = 1$ for any constant and any variable, $|(t \cdot s)| = |(t + s)| = |t| + |s| + 1$, $|!t| = |t| + 1$.

Lemma 6 (Encoding the Hypothetical Syllogism Rule). *The operation*

$$\mathrm{syl}(t, s) = \big(c_2 \cdot (c_1 \cdot s)\big) \cdot t$$

with $|\mathrm{syl}(t, s)| = |t| + |s| + 5$ *encodes the Hypothetical Syllogism Rule, i.e.,*

$$\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{syl}(t, s) : H \quad \Longleftrightarrow \quad \begin{array}{l} H = A \to C \text{ such that for some } B \\ \mathsf{rLP}_{\mathcal{CS}} \vdash t : (A \to B) \quad \text{and} \quad \mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C). \end{array}$$

Proof. ($\Longleftarrow$). Here is a derivation of $t : (A \to B), s : (B \to C) \vdash \mathrm{syl}(t, s) : (A \to C)$:

$$\begin{array}{rcll}
c_1 & : & ((B \to C) \to (A \to (B \to C))) & (*\mathcal{CS}) \\
s & : & (B \to C) & (\text{Hyp}) \\
c_1 \cdot s & : & (A \to (B \to C)) & (*\text{A2}) \\
c_2 & : & ((A \to (B \to C)) \to ((A \to B) \to (A \to C))) & (*\mathcal{CS}) \\
c_2 \cdot (c_1 \cdot s) & : & ((A \to B) \to (A \to C)) & (*\text{A2}) \\
t & : & (A \to B) & (\text{Hyp}) \\
(c_2 \cdot (c_1 \cdot s)) \cdot t & : & (A \to C) & (*\text{A2})
\end{array}$$

($\Longrightarrow$). Consider an arbitrary derivation of $\mathrm{syl}(t, s) : H$ in the $*$-calculus. It can easily be seen that any such derivation must have the same structure as the one used for the $\Longleftarrow$-direction above: the only difference can be in the choice of axioms for constants c_1 and c_2 and of formulas for terms s and t. Since $\mathcal{CS}$ is schematically injective, we know the form of axioms proven by c_1 and c_2. Thus, we can shape this as a unification problem: find X_1, Y_1, X_2, Y_2, Z_2, X_s, and X_t

such that $\mathsf{rLP}_{\mathcal{CS}} \vdash s : X_s$, $\mathsf{rLP}_{\mathcal{CS}} \vdash t : X_t$, and the following is a $*$-calculus derivation of $s : X_s, t : X_t \vdash \mathrm{syl}(t, s) : H$:

1.	$c_1 : (X_1 \to (Y_1 \to X_1))$	$(*\mathcal{CS})$
2.	$s : X_s$	(Hyp)
3.	$c_1 \cdot s : (Y_1 \to X_1)$	$(*\mathrm{A2})$
4.	$c_2 : ((X_2 \to (Y_2 \to Z_2)) \to ((X_2 \to Y_2) \to (X_2 \to Z_2)))$	$(*\mathcal{CS})$
5.	$c_2 \cdot (c_1 \cdot s) : ((X_2 \to Y_2) \to (X_2 \to Z_2))$	$(*\mathrm{A2})$
6.	$t : X_t$	(Hyp)
7.	$(c_2 \cdot (c_1 \cdot s)) \cdot t : H$	$(*\mathrm{A2})$

To make the applications of rule $*$A2 work in lines 3, 5, and 7, the unification variables have to satisfy the following equations:

$$X_1 = X_s \qquad \text{from 3.} \tag{1}$$
$$X_2 \to (Y_2 \to Z_2) = Y_1 \to X_1 \qquad \text{from 5.} \tag{2}$$
$$X_2 \to Y_2 = X_t \qquad \text{from 7.} \tag{3}$$
$$X_2 \to Z_2 = H \qquad \text{from 7.} \tag{4}$$

By (1) and (2), $X_s = X_1 = Y_2 \to Z_2$. This equation combined with (3) and (4) shows that H is indeed an implication that follows by HS from X_t and X_s justified by t and s respectively. □

Lemma 7 (Stripping k conjunctions). *For any integer $k \geq 0$ there exists a term t_k of size $O(k)$ that encodes the operation of stripping k conjunctions, i.e.,*

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_k : D \qquad \Longleftrightarrow \qquad D = H \to C, \text{ where } C \text{ is a } k\text{-conjunct of } H.$$

Proof. We prove by induction on k that the conditions are satisfied for

$$t_0 = (c_2 \cdot c_1) \cdot c_1 \ ,$$
$$t_{k+1} = \mathrm{syl}(c_{\wedge 1} + c_{\wedge 2}, t_k) \ .$$

It is clear that $|t_k| = 8k + 5$ because $|t_0| = 5$ and $|t_{k+1}| = |t_k| + 8$.

Base case, $k = 0$. ($\Longleftarrow$). If C is a 0-conjunct of H, then $H = C$, and it is easy to see that t_0 corresponds to the standard derivation of the tautology $C \to C$. ($\Longrightarrow$). Any $*$-derivation of $t_0 : D$ must have the form:

1.	$c_2 : ((X_2 \to (Y_2 \to Z_2)) \to ((X_2 \to Y_2) \to (X_2 \to Z_2)))$	$(*\mathcal{CS})$
2.	$c_1 : (X_1 \to (Y_1 \to X_1))$	$(*\mathcal{CS})$
3.	$c_2 \cdot c_1 : ((X_2 \to Y_2) \to (X_2 \to Z_2))$	$(*\mathrm{A2})$
4.	$c_1 : (X_3 \to (Y_3 \to X_3))$	$(*\mathcal{CS})$
5.	$(c_2 \cdot c_1) \cdot c_1 : D$	$(*\mathrm{A2})$

For $*$A2 from line 5 to be valid, it is necessary that $D = X_2 \to Z_2$. It follows from $*$A2 in line 3 that $X_2 \to (Y_2 \to Z_2) = X_1 \to (Y_1 \to X_1)$, in which case $X_2 = X_1 = Z_2$. Therefore, $D = X_2 \to X_2$, which is an implication from a formula to its 0-conjunct.

Induction step. ($\Longleftarrow$). Let H be a formula with a $(k+1)$-conjunct C. Then H must be of the form $H_1 \land H_2$ with C being a k-conjunct of H_i for some $i = 1, 2$. By the induction hypothesis, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_k : (H_i \to C)$ for this i. Since, in addition, $\mathsf{rLP}_{\mathcal{CS}} \vdash c_{\land 1} : (H \to H_1)$ and $\mathsf{rLP}_{\mathcal{CS}} \vdash c_{\land 2} : (H \to H_2)$, by rule $*$A3, $\mathsf{rLP}_{\mathcal{CS}} \vdash (c_{\land 1} + c_{\land 2}) : (H \to H_i)$ for both $i = 1$ and $i = 2$. Then, by Lemma 6, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k+1} : (H \to C)$.
($\Longrightarrow$). By the induction hypothesis, t_k justifies only implications from a formula to one of its k-conjuncts. It is clear from rule $*$A3 that $c_{\land 1} + c_{\land 2}$ justifies only implications from a formula to one of its 1-conjuncts. By Lemma 6, t_{k+1} justifies only hypothetical syllogisms obtained from the latter and the former, but a k-conjunct of a 1-conjunct of a formula is its $(k+1)$-conjunct. □

Lemma 8. *For any term s and any integer $l \geq 0$ there exists a term* $\mathrm{conj}(s, l)$ *of size $O(|s|2^l)$ with the following property:*

$$\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{conj}(s, l) : D \qquad \Longleftrightarrow \qquad \begin{array}{l} D = B \to C_1 \land \cdots \land C_{2^l} \text{ such that} \\ \mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C_i) \text{ for all } i = 1, \ldots, 2^l. \end{array}$$

Proof. We prove by induction on l that the conditions are satisfied for

$$\begin{aligned} \mathrm{conj}(s, 0) &= \mathrm{syl}(s, t_0) \ , \\ \mathrm{conj}(s, l+1) &= \Big(c_2 \cdot \mathrm{syl}\big(\mathrm{conj}(s, l), c_\land\big)\Big) \cdot \mathrm{conj}(s, l) \ . \end{aligned}$$

It is not hard to see that $|\mathrm{conj}(s, l)| = 2^l(|s|+19)-9$ because $|\mathrm{conj}(s, 0)| = |s|+10$ and $|\mathrm{conj}(s, l+1)| = 2|\mathrm{conj}(s, l)| + 9$.

Base case, $l = 0$. ($\Longleftarrow$). For any C, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_0 : (C \to C)$ by Lemma 7. Then, by Lemma 6, $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C)$ implies $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{syl}(s, t_0) : (B \to C)$.
($\Longrightarrow$). By Lemma 6, $\mathrm{syl}(s, t_0)$ justifies only implications $B \to C$ for which there exists an A such that $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to A)$ and $\mathsf{rLP}_{\mathcal{CS}} \vdash t_0 : (A \to C)$. By Lemma 7, the latter implies $A = C$. Therefore, $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C)$.[6]

Induction step. ($\Longleftarrow$). Let $H = C_1 \land \cdots \land C_{2^{l+1}}$ with $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C_i)$ for all its $(l+1)$-conjuncts. Then $H = H_1 \land H_2$ where $C_1, C_2, \ldots, C_{2^l}$ are l-conjuncts of H_1 and $C_{2^l+1}, C_{2^l+2}, \ldots, C_{2^{l+1}}$ are l-conjuncts of H_2. By the induction hypothesis,

$$\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{conj}(s, l) : (B \to H_1) \ , \tag{5}$$

$$\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{conj}(s, l) : (B \to H_2) \ . \tag{6}$$

In addition, $\mathsf{rLP}_{\mathcal{CS}} \vdash c_\land : (H_1 \to (H_2 \to H_1 \land H_2))$; in other words,

$$\mathsf{rLP}_{\mathcal{CS}} \vdash c_\land : (H_1 \to (H_2 \to H)) \ . \tag{7}$$

From (7) and (5) by Lemma 6, for $s' = \mathrm{syl}(\mathrm{conj}(s, l), c_\land)$ we have

$$\mathsf{rLP}_{\mathcal{CS}} \vdash s' : (B \to (H_2 \to H)) \ .$$

[6] Note that, in general, $\mathrm{conj}(s, 0) = s$ does not satisfy the $\Longrightarrow$-direction.

Then, from (6) and $\mathsf{rLP}_{\mathcal{CS}} \vdash c_2 : ((B \to (H_2 \to H)) \to ((B \to H_2) \to (B \to H)))$:

$$\mathsf{rLP}_{\mathcal{CS}} \vdash c_2 \cdot s' : ((B \to H_2) \to (B \to H)) \qquad \text{and, finally,}$$
$$\mathsf{rLP}_{\mathcal{CS}} \vdash (c_2 \cdot s') \cdot \mathrm{conj}(s, l) : (B \to H) \ .$$

It remains to note that $\mathrm{conj}(s, l+1) = (c_2 \cdot s') \cdot \mathrm{conj}(s, l)$.
($\Longrightarrow$). By Lemma 6, the rule

$$\frac{t : (A \to B) \quad s : (B \to C)}{\mathrm{syl}(t, s) : (A \to C)} (\mathrm{Syl})$$

is admissible in the $*$-calculus. So any $*$-derivation of $\mathrm{conj}(s, l+1) : D$ must contain the following key elements (we have already incorporated the induction hypothesis about $\mathrm{conj}(s, l)$ as well as Lemma 6):

1.	$\mathrm{conj}(s, l) : (B \to C_1 \wedge C_2 \wedge \cdots \wedge C_{2^l})$	(IH)
2.	$c_\wedge : (X_\wedge \to (Y_\wedge \to X_\wedge \wedge Y_\wedge))$	$(*\mathcal{CS})$
3.	$s' : (B \to (Y_\wedge \to X_\wedge \wedge Y_\wedge))$	(Syl)
4.	$c_2 : ((X_2 \to (Y_2 \to Z_2)) \to ((X_2 \to Y_2) \to (X_2 \to Z_2)))$	$(*\mathcal{CS})$
5.	$c_2 \cdot s' : ((X_2 \to Y_2) \to (X_2 \to Z_2))$	$(*\mathrm{A2})$
6.	$\mathrm{conj}(s, l) : (B' \to C_{2^l+1} \wedge C_{2^l+2} \wedge \cdots \wedge C_{2^{l+1}})$	(IH)
7.	$(c_2 \cdot s') \cdot \mathrm{conj}(s, l) : D$	$(*\mathrm{A2})$

where $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C_i)$ and $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B' \to C_{2^l+i})$ for $i = 1, \ldots, 2^l$. Let us collect all unification equations necessary for this to be a valid fragment of a $*$-derivation:

$$C_1 \wedge C_2 \wedge \cdots \wedge C_{2^l} = X_\wedge \qquad \text{from 3.} \qquad (8)$$
$$B \to (Y_\wedge \to X_\wedge \wedge Y_\wedge) = X_2 \to (Y_2 \to Z_2) \qquad \text{from 5.} \qquad (9)$$
$$B' \to C_{2^l+1} \wedge C_{2^l+2} \wedge \cdots \wedge C_{2^{l+1}} = X_2 \to Y_2 \qquad \text{from 7.} \qquad (10)$$
$$X_2 \to Z_2 = D \qquad \text{from 7.} \qquad (11)$$

By (9) and (10), $B = X_2 = B'$. Thus, $\mathsf{rLP}_{\mathcal{CS}} \vdash s : (B \to C_i)$ for $i = 1, \ldots, 2^{l+1}$. Also

$$Y_\wedge = Y_2 = C_{2^l+1} \wedge C_{2^l+2} \wedge \cdots \wedge C_{2^{l+1}} \ ,$$

again by (9) and (10). So, by (8) and (9),

$$Z_2 = X_\wedge \wedge Y_\wedge = (C_1 \wedge C_2 \wedge \cdots \wedge C_{2^l}) \wedge (C_{2^l+1} \wedge C_{2^l+2} \wedge \cdots \wedge C_{2^{l+1}}) \ .$$

By (11), D is indeed an implication from B to this balanced conjunction for all of whose $(l+1)$-conjuncts term s justifies their entailment from B. □

Lemma 9. *For the term* $\mathrm{disj} = c_{\vee 1} + c_{\vee 2}$ *of size* $O(1)$,

$$\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{disj} : D \qquad \Longleftrightarrow \qquad D = B \to H, \text{ where } B \text{ is a disjunct of } H.$$

Proof. Easily follows from $*\mathrm{A3}$ and $*\mathcal{CS}$. □

4 Reduction from Vertex Cover, Part I

We now use the justification terms from the previous section to build a polynomial-time many-one reduction from BVC to $\mathsf{rLP}_{\mathcal{CS}}$. In this section, it is sufficient for $\mathcal{CS}$ to be schematic and axiomatically appropriate.

Lemma 10. *Let a term of size $O(k2^l)$ be defined by*

$$t_{k\to l} = \mathrm{conj}(t_k, l) \ .$$

For any binary exponential graph $G = \langle V, E\rangle$ with $|V| = 2^k$ and any set $C \subseteq V$ of size 2^l,

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l} : (F_V \to F_C) \ .$$

Proof. $|\mathrm{conj}(t_k, l)| = O\left(|t_k|2^l\right) = O(k2^l)$.

All l-conjuncts p_i of F_C, where $i \in C$, must be k-conjuncts of F_V. Thus, for any of them by Lemma 7, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_k : (F_V \to p_i)$. Now, by Lemma 8, we have $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{conj}(t_k, l) : (F_V \to F_C)$. □

Lemma 11. *Let a term of size $O(l)$ be defined by*

$$t_{l\to\mathrm{edge}} = \mathrm{syl}(t_l, \mathrm{disj}) \ .$$

For any binary exponential graph $G = \langle V, E\rangle$, any set $C \subseteq V$ of size 2^l, and any edge $e \in E$,

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{l\to\mathrm{edge}} : (F_C \to F_e) \qquad \Longleftrightarrow \qquad e \text{ is covered by } C.$$

Proof. $|\mathrm{syl}(t_l, \mathrm{disj})| = |t_l| + |\mathrm{disj}| + 5 = O(l) + O(1) = O(l)$.
($\Longleftarrow$). If $i \in e \cap C$ is the vertex in C that covers e, then p_i is a disjunct of F_e, so $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{disj} : (p_i \to F_e)$ by Lemma 9. But p_i is also an l-conjunct of F_C, so, by Lemma 7, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_l : (F_C \to p_i)$. Finally, $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{syl}(t_l, \mathrm{disj}) : (F_C \to F_e)$ by Lemma 6.
($\Longrightarrow$). If C does not cover e, it is easy to see that $F_C \to F_e$ is not valid, therefore, $\mathsf{rLP}_{\mathcal{CS}} \nvdash s : (F_C \to F_e)$ for any term s. □

Lemma 12. *Let a term of size $O(l2^m)$ be defined by*

$$s_{l\to m} = \mathrm{conj}(t_{l\to\mathrm{edge}}, m) \ .$$

For any binary exponential graph $G = \langle V, E\rangle$ with $|E| = 2^m$ and any set $C \subseteq V$ of size 2^l,

$$\mathsf{rLP}_{\mathcal{CS}} \vdash s_{l\to m} : (F_C \to F_G) \qquad \Longleftrightarrow \qquad C \text{ is a vertex cover for } G.$$

Proof. $|\mathrm{conj}(t_{l\to\mathrm{edge}}, m)| = O(|t_{l\to\mathrm{edge}}|2^m) = O(l2^m)$.
($\Longleftarrow$). If C is a vertex cover, then $\mathsf{rLP}_{\mathcal{CS}} \vdash t_{l\to\mathrm{edge}} : (F_C \to F_e)$ for all $e \in E$, by Lemma 11. All m-conjuncts of F_G are F_e's with $e \in E$. Hence, by Lemma 8, $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{conj}(t_{l\to\mathrm{edge}}, m) : (F_C \to F_G)$.
($\Longrightarrow$). If C is not a vertex cover, by Lemma 5.3, formula $F_C \to F_G$ is not valid, hence $\mathsf{rLP}_{\mathcal{CS}} \nvdash s : (F_C \to F_G)$ for any term s. □

Theorem 13. *Let a term of size $O(k2^l) + O(l2^m)$ be defined by*

$$t_{k\to l\to m} = \mathrm{syl}(t_{k\to l}, s_{l\to m}) \ .$$

For any binary exponential graph $G = \langle V, E\rangle$ with $|V| = 2^k$ and $|E| = 2^m$ and any integer $0 \leq l \leq k$,

$$G \text{ has a vertex cover of size} \leq 2^l \quad \Longrightarrow \quad \mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l\to m} : (F_V \to F_G) \ .$$

Proof. $|\mathrm{syl}(t_{k\to l}, s_{l\to m})| = |t_{k\to l}| + |s_{l\to m}| + 5 = O(k2^l) + O(l2^m)$.

By Lemma 10, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l} : (F_V \to F_C)$ for any set $C \subseteq V$ of size 2^l. If G has a vertex cover of size $\leq 2^l$, it can be enlarged to a vertex cover of size 2^l. Let C be such a vertex cover of size 2^l. Then, by Lemma 12, $\mathsf{rLP}_{\mathcal{CS}} \vdash s_{l\to m} : (F_C \to F_G)$. Thus, by Lemma 6, $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{syl}(t_{k\to l}, s_{l\to m}) : (F_V \to F_G)$. □

Note that the term $t_{k\to l\to m}$ depends only on size 2^l of a vertex cover C and the numbers of vertices and edges of G.

5 Reduction from Vertex Cover, Part II

Earlier, we promised to show that the choice of a particular axiomatization for the propositional logic has no impact on our results. Indeed, for all results in Sect. 4 as well as for the $\Longleftarrow$-directions in Sect. 3, any finite schematic axiomatization would suffice. For an alternative set of propositional axiom schemes, the constants would simply be replaced by corresponding ground terms that justify the former axioms in the new system. These new terms would have size $O(1)$. It follows from the proof of Theorem 13 that the derivation of $F_V \to F_G$ we intended to represent by term $t_{k\to l\to m}$ fails. We use the condition of schematic injectivity to make sure that no other derivation of tautology $F_V \to F_G$ accidentally falls under the scope of $t_{k\to l\to m}$. In doing so, it is instrumental that we can provide a term (not necessarily a constant) that justifies all tautologies from a particular scheme and only them. Although non-atomic terms containing + typically justify several schemes of formulas even if $\mathcal{CS}$ is schematically injective, it is possible to justify all propositional tautologies by +-free terms (see [Art01]), which justify at most one scheme. Using this observation, it is not hard to show that our results (including the ones to follow in this section) are, in fact, independent of the propositional axiom schemes chosen for A1.

To finish the polynomial-time reduction from BVC to $\mathsf{rLP}_{\mathcal{CS}}$ it now remains to prove the other direction:

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l\to m} : (F_V \to F_G) \quad \Longrightarrow \quad G \text{ has a vertex cover of size} \leq 2^l.$$

In this section, we again need the strongest restrictions on $\mathcal{CS}$: to be axiomatically appropriate and schematically injective.

Lemma 14 (Converse to Lemma 10).

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l} : H \quad \Longrightarrow \quad \begin{array}{l} H = B \to D, \\ \textit{where } D \textit{ is a balanced conjunction of depth} \geq l \\ \textit{whose all } l\textit{-conjuncts are } k\textit{-conjuncts of } B. \end{array}$$

Proof. By definition, $t_{k\to l} = \mathrm{conj}(t_k, l)$, so by Lemma 8, it justifies only implications $B \to C_1 \wedge \cdots \wedge C_{2^l}$ with $\mathsf{rLP}_{\mathcal{CS}} \vdash t_k : (B \to C_i)$ for $i = 1, \ldots, 2^l$. By Lemma 7, term t_k only justifies implications from a formula to its k-conjuncts. □

Lemma 15 (Converse to Lemma 11).

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{l\to\mathrm{edge}} : H \quad \Longrightarrow \quad \begin{array}{l} H = B \to D_1 \vee D_2, \\ \textit{where either } D_1 \textit{ or } D_2 \textit{ is an } l\textit{-conjunct of } B. \end{array}$$

Proof. By definition, $t_{l\to\mathrm{edge}} = \mathrm{syl}(t_l, \mathrm{disj})$. By Lemma 6, H can only be an implication $B \to D$ such that $\mathsf{rLP}_{\mathcal{CS}} \vdash t_l : (B \to C)$ and $\mathsf{rLP}_{\mathcal{CS}} \vdash \mathrm{disj} : (C \to D)$ for some C. By Lemma 9, the latter statement implies that $D = D_1 \vee D_2$ with $C = D_i$ for some $i = 1, 2$. By Lemma 7, D_i is an l-conjunct of B. □

Lemma 16 (Converse to Lemma 12).

$$\mathsf{rLP}_{\mathcal{CS}} \vdash s_{l\to m} : H \quad \Longrightarrow \quad \begin{array}{l} H = B \to (C_1 \vee D_1) \wedge \cdots \wedge (C_{2^m} \vee D_{2^m}), \\ \textit{where either } C_i \textit{ or } D_i \textit{ is an } l\textit{-conjunct of } B \\ \textit{for each } i = 1, \ldots, 2^m. \end{array}$$

Proof. By definition, $s_{l\to m} = \mathrm{conj}(t_{l\to\mathrm{edge}}, m)$. By Lemma 8, H must be an implication from some B to a balanced conjunction of depth $\geq m$ such that, for all its m-conjuncts F, $\mathsf{rLP}_{\mathcal{CS}} \vdash t_{l\to\mathrm{edge}} : (B \to F)$. By Lemma 15, each of these m-conjuncts must be a disjunction with one of the disjuncts being an l-conjunct of B. □

Theorem 17 (Converse to Theorem 13).

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l\to m} : H \quad \Longrightarrow \quad \begin{array}{l} H = B \to (C_1 \vee D_1) \wedge \cdots \wedge (C_{2^m} \vee D_{2^m}), \\ \textit{and there is a size } \leq 2^l \textit{ set } X \textit{ of } k\textit{-conjuncts of } B \\ \textit{with either } C_i \in X \textit{ or } D_i \in X \textit{ for each } i = 1, \ldots, 2^m. \end{array}$$

Proof. By definition, $t_{k\to l\to m} = \mathrm{syl}(t_{k\to l}, s_{l\to m})$. By Lemma 6, $H = B \to F$ with (a) $\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l} : (B \to Q)$, (b) $\mathsf{rLP}_{\mathcal{CS}} \vdash s_{l\to m} : (Q \to F)$ for some Q. From (a), by Lemma 14, $Q = Q_1 \wedge \cdots \wedge Q_{2^l}$ whose all l-conjuncts Q_i's are also k-conjuncts of B. So $X = \{Q_i \mid i = 1, \ldots, 2^l\}$ is a size $\leq 2^l$ set (with possible repetitions) of k-conjuncts of B. It follows now from (b), by Lemma 16, that $F = (C_1 \vee D_1) \wedge \cdots \wedge (C_{2^m} \vee D_{2^m})$ with either C_i or D_i being an l-conjunct of Q for each $i = 1, \ldots, 2^m$, i.e., with either $C_i \in X$ or $D_i \in X$ for each $i = 1, \ldots, 2^m$. □

Theorem 18. *For any binary exponential graph $G = \langle V, E\rangle$ with $|V| = 2^k$ and $|E| = 2^m$ and any integer $0 \leq l \leq k$,*

$$\mathsf{rLP}_{\mathcal{CS}} \vdash t_{k\to l\to m} : (F_V \to F_G) \quad \Longleftrightarrow \quad G \textit{ has a vertex cover of size } \leq 2^l.$$

Proof. The $\Longleftarrow$-direction was proven in Theorem 13. We now prove the $\Longrightarrow$-direction. $F_V \to F_G$ already has the form prescribed by Theorem 17. The only

k-conjuncts of F_V are sentence letters $p_1, \ldots, p_{2^k}$. Therefore, there must exist a set X of $\leq 2^l$ of these sentence letters such that for each m-conjunct F_e of F_G at least one of its disjuncts, $p_{v_1(e)}$ or $p_{v_2(e)}$, is in X. This literally means that in G there is a set of $\leq 2^l$ vertices that covers all edges. □

Theorem 19. *For an axiomatically appropriate and schematically injective $\mathcal{CS}$, derivability in $\mathsf{rLP}_{\mathcal{CS}}$ is NP-complete.*

Proof. It was proven in [Kru03] that $\mathsf{rLP}_{\mathcal{CS}}$ is in NP. It is easy to see that both F_V and F_G have size polynomial in the size of G. As for term $t_{k\to l\to m}$, it was shown in Theorem 13 that $|t_{k\to l\to m}| = O(k2^l) + O(l2^m)$, which is polynomial in the size of G provided $l \leq k$ (BVC for $l > k$ is trivial). Thus, Theorem 18 shows that $\mathsf{rLP}_{\mathcal{CS}}$ is NP-hard. □

6 Other Justification Logics

Justification counterparts J, JD, JT, $\mathsf{J4}$, and $\mathsf{JD4}$ of modal logics K, D, T, $\mathsf{K4}$, and $\mathsf{D4}$ respectively have been developed in [Bre00] (see also [Art08a]). In addition, there are several hybrid logics combining justifications and epistemic modalities for multiple agents: $\mathsf{T}_n\mathsf{LP}_{\mathcal{CS}}$, $\mathsf{S4}_n\mathsf{LP}_{\mathcal{CS}}$, and $\mathsf{S5}_n\mathsf{LP}_{\mathcal{CS}}$ (see [Art06]). It was shown in [Kuz08a] that their reflected fragments $\mathsf{rJ4}_{\mathcal{CS}}$, $\mathsf{rJD4}_{\mathcal{CS}}$, $\mathsf{rT}_n\mathsf{LP}_{\mathcal{CS}}$, $\mathsf{rS4}_n\mathsf{LP}_{\mathcal{CS}}$, and $\mathsf{rS5}_n\mathsf{LP}_{\mathcal{CS}}$ are axiomatized by the same $*$-calculus as $\mathsf{rLP}_{\mathcal{CS}}$, whereas axiomatization for $\mathsf{rJ}_{\mathcal{CS}}$, $\mathsf{rJD}_{\mathcal{CS}}$, and $\mathsf{rJT}_{\mathcal{CS}}$ is obtained by dropping $*$A5 for arbitrary terms while simultaneously integrating it into $*\mathcal{CS}$ for constants. This immediately yields that the Derivability Problem for all these logics is in NP for any schematic $\mathcal{CS}$ (see [Kuz08a]).

For lack of space, we cannot provide sufficient details here; we will just mention that hybrid logics $\mathsf{rT}_n\mathsf{LP}_{\mathcal{CS}}$, $\mathsf{rS4}_n\mathsf{LP}_{\mathcal{CS}}$, and $\mathsf{rS5}_n\mathsf{LP}_{\mathcal{CS}}$ are conservative over $\mathsf{rLP}_{\mathcal{CS}'}$, where $\mathcal{CS}'$ is the modality-free part of $\mathcal{CS}$. On the other hand, $\mathsf{rJ}_{\mathcal{CS}}$, $\mathsf{rJD}_{\mathcal{CS}}$, $\mathsf{rJT}_{\mathcal{CS}}$, $\mathsf{rJ4}_{\mathcal{CS}}$, and $\mathsf{rJD4}_{\mathcal{CS}}$ are strictly weaker than $\mathsf{rLP}_{\mathcal{CS}}$, but all the reasoning involved in constructing term $t_{k\to l\to m}$ can easily be performed in them too.

Theorem 20. *For an axiomatically appropriate and schematically injective constant specification $\mathcal{CS}$, the Derivability Problem for $\mathsf{rJ}_{\mathcal{CS}}$, $\mathsf{rJD}_{\mathcal{CS}}$, $\mathsf{rJT}_{\mathcal{CS}}$, $\mathsf{rJ4}_{\mathcal{CS}}$, $\mathsf{rJD4}_{\mathcal{CS}}$, $\mathsf{rT}_n\mathsf{LP}_{\mathcal{CS}}$, $\mathsf{rS4}_n\mathsf{LP}_{\mathcal{CS}}$, and $\mathsf{rS5}_n\mathsf{LP}_{\mathcal{CS}}$ is NP-complete.*

Acknowledgments.

We are grateful to Sergei Artemov for playing the role of a catalyst for this research project. We thank the anonymous referees for their comments.

References

[AK06] Sergei [N.] Artemov and Roman Kuznets. Logical omniscience via proof complexity. In Zoltán Ésik, editor, *Computer Science Logic, 20th International Workshop, CSL 2006, 15th Annual Conference of the EACSL, Szeged,*

Hungary, September 25–29, 2006, Proceedings, volume 4207 of *Lecture Notes in Computer Science*, pages 135–149. Springer, 2006.

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

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

[Art06] Sergei [N.] Artemov. Justified common knowledge. *Theoretical Computer Science*, 357(1–3):4–22, July 2006.

[Art08a] Sergei [N.] Artemov. The logic of justification. Technical Report TR–2008010, CUNY Ph.D. Program in Computer Science, September 2008.

[Art08b] Sergei [N.] Artemov. Why do we need Justification Logic? Technical Report TR–2008014, CUNY Ph.D. Program in Computer Science, September 2008.

[BB93] Maria Luisa Bonet and Samuel R. Buss. The deduction rule and linear and near-linear proof simulations. *Journal of Symbolic Logic*, 58(2):688–709, June 1993.

[Bre00] Vladimir N. Brezhnev. On explicit counterparts of modal logics. Technical Report CFIS 2000–05, Cornell University, 2000.

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

[Kru06] Nikolai V. Krupski. On the complexity of the reflected logic of proofs. *Theoretical Computer Science*, 357(1–3):136–142, July 2006.

[Kuz00] Roman Kuznets. On the complexity of explicit modal logics. In Peter G. Clote and Helmut Schwichtenberg, editors, *Computer Science Logic, 14th International Workshop, CSL 2000, Annual Conference of the EACSL, Fischbachau, Germany, August 21–26, 2000, Proceedings*, volume 1862 of *Lecture Notes in Computer Science*, pages 371–383. Springer, 2000. Errata concerning the explicit counterparts of $\mathcal{D}$ and $\mathcal{D}4$ are published as [Kuz08b].

[Kuz08a] Roman Kuznets. *Complexity Issues in Justification Logic*. PhD thesis, CUNY Graduate Center, May 2008.

[Kuz08b] Roman Kuznets. Complexity through tableaux in justification logic. In *Abstracts of Plenary Talks, Tutorials, Special Sessions, Contributed Talks of Logic Colloquium 2008 (LC'08)*, pages 38–39, Bern, Switzerland, July 3–8, 2008. Abstract.

[Kuz08c] Roman Kuznets. Self-referentiality of justified knowledge. In Edward A. Hirsch, Alexander A. Razborov, Alexei Semenov, and Anatol Slissenko, editors, *Third International Computer Science Symposium in Russia, CSR 2008, Moscow, Russia, June 7–12, 2008, Proceedings*, volume 5010 of *Lecture Notes in Computer Science*, pages 228–239. Springer, 2008.

[Lad77] Richard E. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal on Computing*, 6(3):467–480, September 1977.

[Mil07] Robert Milnikel. Derivability in certain subsystems of the Logic of Proofs is Π_2^p-complete. *Annals of Pure and Applied Logic*, 145(3):223–239, March 2007.