2006

TR-2006005: Logical Omniscience via Proof Complexity

Sergei Artemov

Roman Kuznets

Logical Omniscience via Proof Complexity

Sergei Artemov and Roman Kuznets*

CUNY Graduate Center
365 Fifth Ave, New York, NY 10016, USA
{SArtemov,RKuznets}@gc.cuny.edu

Abstract. The Hintikka-style modal logic approach to knowledge has a well-known defect of logical omniscience, i.e., an unrealistic feature that an agent knows all logical consequences of her assumptions. In this paper we suggest the following Logical Omniscience Test (LOT): an epistemic system E is not logically omniscient if for any valid in E knowledge assertion $\mathcal{A}$ of type '*F is known*' there is a proof of F in E, the complexity of which is bounded by some polynomial in the length of $\mathcal{A}$. We show that the usual epistemic modal logics are logically omniscient (modulo some common complexity assumptions). We also apply LOT to Justification Logic, which along with the usual knowledge operator $K_i(F)$ ('*agent i knows F*') contain evidence assertions $t{:}F$ ('*t is a justification for F*'). In Justification Logic, the evidence part is an appropriate extension of the Logic of Proofs LP, which guarantees that the collection of evidence terms t is rich enough to match modal logic. We show that justification logic systems are logically omniscient w.r.t. the usual knowledge and are not logically omniscient w.r.t. the evidence-based knowledge.

1 Introduction

The modal logic approach to knowledge [26] has a well-known defect of logical omniscience, i.e., an unrealistic feature that an agent knows all logical consequences of her assumptions. This does not seem to correspond to the reasoning capabilities of either a human being or a computer. In particular, a logically omniscient agent would know whether White has a non-losing strategy in chess provided that the agent knows the rules of chess. This assumption is certainly not true of any reasoning entity known.

The logical omniscience problem, raised in [15, 16, 27, 39, 41], has been studied extensively in logic, epistemology, game theory and economics, distributed systems, artificial intelligence, etc., in a large number of papers, including [1, 10, 14–17, 23, 24, 28, 34, 37, 38, 42, 43, 45–48], and many others. Most of them adjust epistemic models to avoid certain features of logical omniscience.

In this paper we try a general approach based on proof complexity to define and test the logical omniscience property of an epistemic system. This approach was inspired by the Cook-Reckhow theory of proof complexity [12, 44].

* The author is supported in part by a Research Grant for Doctoral Students from CUNY Graduate Center

We see the essence of the logical omniscience problem in a nonconstructive character of modal languages which are able to symbolically represent knowledge without providing any information about its origin. In a modal language, there are valid knowledge assertions which do not have feasible justifications, hence cannot be regarded valid in any practical sense. So, for us logical omniscience is rather a syntactic and complexity issue. On the basis of this understanding we suggest the following test:

> an epistemic system E is *not logically omniscient* if for any valid in E knowledge assertion $\mathcal{A}$ of type *F is known* there is a proof of F in E, the complexity of which is bounded by some polynomial in the length of $\mathcal{A}$.

We show that the traditional epistemic modal logics do not pass this test, hence are logically omniscient. This complies nicely with the intuition that led to a recognition of the logical omniscience problem in the first place.

The aforementioned test suggests ways of building epistemic systems which are not logically omniscient: one has to alter the syntax of knowledge assertions *F is known* in order to include more information about **why** *F is known*. This added information should be sufficient for recovering a certified justification, e.g. a feasible proof, for F.

We show that recently introduced systems of Justification Logic from [3–5, 7, 9], are not logically omniscient.

In Sect. 2, we formally introduce the Logical Omniscience Test (LOT). In Sect. 3 we prove that, according to LOT, the traditional epistemic modal logics are logically omniscient. Then in Sect. 4 we formulate the system LP, which is a general purpose calculus of evidence terms, and show in Sect. 5 that LP as an epistemic system is not logically omniscient. Finally, in Sect. 6 we extend these results to the multi-agent logics with common knowledge and corresponding evidence-based knowledge systems.

2 Logical Omniscience Test

Let L be a logical theory. According to Cook and Reckhow (cf. [12, 44]), a *proof system* for L is a polynomial-time computable function $p\colon \Sigma^* \to \mathsf{L}$ from the set of strings in some alphabet, called proofs, onto the set of L-valid formulas. In addition we consider a measure of size for proofs which is a function $\ell\colon \Sigma^* \to \mathbb{N}$, and a measure of size for individual formulas $|\cdot|\colon \mathrm{Fm}_{\mathsf{L}} \to \mathbb{N}$.

Logical Omniscience Test (Artemov, 2005). *Let L be a theory capable of expressing knowledge assertions 'formula F is known,' supplied with a proof system p, a measure of size for proofs ℓ, and a measure of size for individual formulas $|\cdot|$. Theory L is* **not logically omniscient** *w.r.t. proof system p under size measures ℓ and $|\cdot|$ if there exists a polynomial P such that, for each valid in L knowledge assertion $\mathcal{A}$ stating that 'F is known,' formula F has a proof $\mathcal{D} \in \Sigma^*$ such that*

$$\ell(\mathcal{D}) \leq P(|\mathcal{A}|) \ .$$

Note 1. This test has a proof system and measures of size for proofs and formulas as parameters. With such a freedom, one should be careful when applying this test to real epistemic systems. In particular, in this paper we consider only complexity measures that are commonly used in proof theory for various specific types of proofs.

In this paper, we mostly consider Hilbert-style proof systems. The size measures commonly associated with them are

1. number of formulas in a derivation, i.e., the number of proof steps,
2. number of logical symbols in a derivation,
3. bit size of a derivation, i.e., number of symbols with the size of indices of propositional variables, etc. taken into account. In other words, this is the string length in alphabet Σ^*.

These are the three measures we will concentrate on. If the size of a proof $\ell(\mathcal{D})$ is the number of symbols (counting or not counting indices), it seems reasonable to use the same measure for the size of formulas, $|F| = \ell(F)$. But in case 1 that would mean $|F| = 1$ for all formulas, which is not a fair measure. So, if the size of a proof is the number of formulas, we will measure the size of individual formulas using number of symbols (again with or without indices). This is the reason why, in general, we need two different measures for proofs and formulas.

3 Modal Epistemic Logics Are Logically Omniscient

It is fairly easy to show that a modal logic, such as $\mathsf{S4}$, is logically omniscient under the bit size measure *w.r.t. any proof system*, modulo a common complexity assumption.

Theorem 1. *Consider any proof system p for $\mathsf{S4}$. Let the size of a proof (a formula) be the string length of that proof (that formula). Then $\mathsf{S4}$ is logically omniscient, unless PSPACE=NP.*

Proof. Indeed, suppose $\mathsf{S4}$ is not logically omniscient, so for every valid knowledge assertion KF, formula F has a polynomial size proof in proof system p, i.e., there exists a polynomial P such that for every $\mathsf{S4} \vdash KF$ there is a proof $\mathcal{D}_F$ of F with $\ell(\mathcal{D}_F) \leq P(|KF|)$.

Then we can construct an NP decision procedure for $\mathsf{S4}$. We have $\mathsf{S4} \vdash G$ iff $\mathsf{S4} \vdash KG$. So to determine whether formula G is valid, non-deterministically guess its polynomial-size proof in proof system p. Then, check that it is indeed a proof of G; this can be done in polynomial time of the size of the proof (by definition of a proof system), which in its turn is a polynomial in $|KG|$.

On the other hand, it is well known that $\mathsf{S4}$ is PSPACE-complete ([31]). Thus, the existence of an NP-algorithm for $\mathsf{S4}$ would ensure that PSPACE$\subseteq$NP, in which case these two classes coincide and the polynomial hierarchy collapses. □

If we restrict our attention to Hilbert-style proofs, there are the other two size measures available. But even if size of the proof is just the number of formulas, we are still able to show that S4 is logically omniscient (modulo non-collapsing of the polynomial hierarchy).

Theorem 2. S4 *is logically omniscient w.r.t. the Hilbert proof system with the size of a proof being the number of formulas in it, unless PSPACE=NP.*

Proof. Again, we want to construct an NP algorithm for the decision problem in S4. But we cannot NP-guess the whole proof. Although there are only polynomially many formulas, still the proof can a priori be exponentially long if the formulas are huge.

We will use unification and modified Robinson's algorithm (see [13]) to do the proof schematically.

Again, for an arbitrary formula G, non-deterministically guess the structure of a Hilbert proof of KG, i.e., for each of the polynomially many formulas guess whether it is an axiom, or a conclusion of a modus ponens rule, or a conclusion of a necessitation rule. For each rule also guess which of the other formulas were used as its premise(s); for each axiom guess which of the finitely many axiom schemes it belongs to. This gives us the structure of the derivation tree, in fact of the derivation dag because in Hilbert proofs one formula can be used in several modus ponens rules.

Write each axiom used in the form of the corresponding axiom scheme using variables over formulas (variables in different axioms must be distinct). Then, starting from the axioms, we can restore the proof in a schematic way. Where a necessitation rule needs to be used, just prefix the formula with K. A case of modus ponens is more interesting. Suppose modus ponens is to be used on schemes $X \to Y$ and Z. Then, unify X with Z using modified Robinson's algorithm from [13] and apply the resulting most general unifier (mgu) to Y.

Eventually, at the root of the tree we will obtain the most general form of formulas that can be proved using derivations with this particular dag structure. Unify this form with formula KG.

All unifications can be done in quadratic time of the size of all the formula dags in the derivation dag, such is the complexity of modified Robinson's algorithm. Each axiom scheme at the beginning has a constant size, and the number of axioms and rules is polynomial in $|KG|$; hence the whole unification procedure is polynomial.

Again we were able to construct an NP decision algorithm under the assumption that there is a polynomial-step Hilbert derivation. □

So S4 turns out to be logically omniscient w.r.t. to an arbitrary proof system under the bit size measure and w.r.t. to Hilbert proofs under any commonly used measure, provided, of course, that the polynomial hierarchy does not collapse.

It is not hard to generalize this result to the epistemic logic $\mathsf{S4}_n$ of n knowledge agents and the logic of common knowledge $\mathsf{S4}_n^{\mathrm{C}}$. The argument is essentially the same, only for $\mathsf{S4}_n^{\mathrm{C}}$ the effect of it not being logically omniscient would be even more devastating: $\mathsf{S4}_n^{\mathrm{C}}$ is EXPTIME-complete (for $n \geq 2$) (see [24]).

Theorem 3. *1.* $\mathsf{S4}_n$ *is logically omniscient w.r.t. an arbitrary proof system under the bit size measure, unless PSPACE=NP.*

2. $\mathsf{S4}_n$ *is logically omniscient w.r.t. the Hilbert proof system with the size of a proof being the number of formulas in it, unless PSPACE=NP.*

3. $\mathsf{S4}_n^{\mathrm{C}}$ *is logically omniscient w.r.t. an arbitrary proof system under the bit size measure, unless EXPTIME=NP.*

4. $\mathsf{S4}_n^{\mathrm{C}}$ *is logically omniscient w.r.t. the Hilbert proof system with the size of a proof being the number of formulas in it, unless EXPTIME=NP.*

There are epistemic logics that are co-NP-complete, e.g. S5. Repeating the argument for them would yield NP=co-NP.

4 Logic of Explicit Knowledge LP

4.1 Axiom System

LP was originally introduced as the Logic of Proofs by Artemov in 1995 (see [2, 3]). Subsequently, in [4–9, 18, 20] LP has been used as a general purpose calculus of evidence, which helped to incorporate justification into formal epistemology thus meeting a long standing demand in this area [11, 21, 22, 25, 32, 33, 35, 40].

Instead of the modal knowledge operator K, the Logic of Proofs LP uses a family of explicit knowledge operators in format $t{:}F$ with the intended meaning "F is known for reason t." Evidence terms t are built from evidence constants c_i and evidence variables x_i by means of three operations: unary ! and binary $+$, $\cdot$

$$t ::= c_i \mid x_i \mid !\,t \mid t \cdot t \mid t + t$$

The axioms of LP_0 are obtained by adding the following schemes to a finite set of axiom schemes of classical propositional logic

LP1	$s{:}(F \to G) \to (t{:}F \to (s \cdot t){:}G)$	(application)
LP2	$t{:}F \to !\,t{:}t{:}F$	(proof checker)
LP3	$s{:}F \to (s+t){:}F, \quad t{:}F \to (s+t){:}F$	(union)
LP4	$t{:}F \to F$	(explicit reflexivity)

The usual way to define the full LP is to add to LP_0 the rule of axiom necessitation:

if A is a propositional axiom or one of LP1-4 *and c is a constant, infer $c{:}A$.*

This definition stresses tight connections between LP and S4 since LP axioms and rules are explicit versions of those of S4. In particular, the axiom necessitation rule is the constructive version of a special case of modal Necessitation Rule limited to axioms only. For the sake of technical convenience in this paper we consider a slightly different but equivalent formulation of LP.

Definition 1. *A* constant specification $\mathcal{CS}$ *is a set of* LP*-formulas of form* $c_i : A$*, where* c_i *is an evidence constant,* A *is an axiom. A constant specification is called* injective *if no two axioms are assigned to the same evidence constant. A constant specification is called* maximal *if each axiom is assigned to every evidence constant.* $\mathsf{LP}_{\mathcal{CS}}$ *is the result of adding constant specification* $\mathcal{CS}$ *as new axioms to* LP_0*.* LP *is* $\mathsf{LP}_{\mathcal{CS}}$ *for the maximal constant specification* $\mathcal{CS}$*.*

The following realization theorem shows that $\mathsf{S4}$ is the forgetful projection of LP (see [3]). We define a forgetful mapping as $(t:F)^\circ = K(F^\circ)$.

Realization Theorem 4. ([2, 3])

1. *If* $\mathsf{LP} \vdash G$*, then* $\mathsf{S4} \vdash G^\circ$*.*
2. *If* $\mathsf{S4} \vdash H$*, then there exists an* LP*-formula* B *(called a realization of* H*) such that* $\mathsf{LP} \vdash B$ *and* $B^\circ = H$*.*

The Realization Theorem shows that each occurrence of epistemic modality K in a modal epistemic principle H can be replaced by some evidence term thus extracting explicit meaning of H. Moreover, it is possible to recover the evidence terms in a Skolem style, namely, by realizing negative occurrences of modality by evidence variables only.

Lifting Lemma 1. ([2, 3]) *If* $\mathsf{LP} \vdash F$*, then there exists a ground*[1]*+-free evidence term* t *such that* $\mathsf{LP} \vdash t:F$*.*

4.2 Epistemic Semantics of Evidence-based Knowledge

Epistemic semantics for LP was introduced by Fitting in ([18, 20]) based on earlier work by Mkrtychev ([36]). Fitting semantics was extended to evidence-based systems with both knowledge modalities K_iF and evidence assertions $t{:}F$ in [4, 5, 7, 9, 8].

Fitting model for LP is a quadruple $\mathcal{M} = (W, R, \mathcal{E}, V)$, where (W, R, V) is the usual $\mathsf{S4}$ Kripke model, and $\mathcal{E}$ is an evidence function defined as follows.

Definition 2. *A* possible evidence function $\mathcal{E}: W \times \mathrm{Tm} \to 2^{\mathrm{Fm}}$ *maps worlds and terms to sets of formulas. An* evidence function *is a possible evidence function* $\mathcal{E}: W \times \mathrm{Tm} \to 2^{\mathrm{Fm}}$ *that satisfies the following conditions:*

1. Monotonicity*:* wRu *implies* $\mathcal{E}(w,t) \subseteq \mathcal{E}(u,t)$
2. Closure*:*
   - Application*:* $(F \to G) \in \mathcal{E}(w,s)$ *and* $F \in \mathcal{E}(w,t)$ *implies* $G \in \mathcal{E}(w, s \cdot t)$
   - Proof Checker*:* $F \in \mathcal{E}(w,t)$ *implies* $t{:}F \in \mathcal{E}(w, !t)$
   - Sum*:* $\mathcal{E}(w,s) \cup \mathcal{E}(w,t) \subseteq \mathcal{E}(w, s+t)$

For a given constant specification $\mathcal{CS}$ *a* $\mathcal{CS}$-evidence function *is an evidence function which respects* $\mathcal{CS}$*:* $c_i : A \in \mathcal{CS}$ *implies* $A \in \mathcal{E}(w, c_i)$*. When speaking about* $\mathcal{CS}$*-evidence functions for the maximal* $\mathcal{CS}$ *(case of* LP*), we will omit prefix* $\mathcal{CS}$ *and will simply call them* evidence functions*.*

[1] *Ground* here means that no evidence variable occurs in it.

Forcing relation $\mathcal{M}, w \Vdash F$ is defined by induction on F.

1. $\mathcal{M}, w \Vdash P$ iff $V(w, P) = t$ for propositional variables P;
2. boolean connectives are classical;
3. $\mathcal{M}, w \Vdash s{:}G$ iff $G \in \mathcal{E}(w, s)$ and $\mathcal{M}, u \Vdash G$ for all wRu.

Again, when speaking about models for LP (case of the maximal $\mathcal{CS}$), we will omit prefix $\mathcal{CS}$ and will simply call them *models* (or *F-models*).

As was shown in [18, 20], $\mathsf{LP}_{\mathcal{CS}}$ is sound and complete with respect to $\mathcal{CS}$-models. Mkrtychev models (M-models) are single-world Fitting models. As was shown in [36], $\mathsf{LP}_{\mathcal{CS}}$ is sound and complete with respect to M-models as well.

We are mostly interested in knowledge assertions $t{:}F$. N. Krupski (see [29]) developed a special calculus for them that will prove useful to us.

Definition 3. *The axioms of* logic $\mathsf{rLP}_{\mathcal{CS}}$ *are exactly the set* $\mathcal{CS}$*. The rules are*

$$\frac{t{:}F}{!\,t{:}t{:}F} \qquad \frac{s{:}F}{(s+t){:}F} \qquad \frac{t{:}F}{(s+t){:}F} \qquad \frac{s{:}(F \to G) \quad t{:}F}{(s \cdot t){:}G}$$

Theorem 5. ([29]) $\mathsf{LP}_{\mathcal{CS}} \vdash t{:}F$ *iff* $\mathsf{rLP}_{\mathcal{CS}} \vdash t{:}F$.

We will again omit subscript $\mathcal{CS}$ when discussing the maximal constant specification.

5 Evidence-Based Knowledge Is Not Logically Omniscient

Now we are ready to show that explicit knowledge avoids logical omniscience. The first question we have to settle is what constitutes a 'knowledge assertion' here. Apparently, the straightforward answer $t{:}F$, generally speaking, is not satisfactory since both t and F may contain evidence constants, the meaning of which is given only in a corresponding constant specification, thus the latter should be a legitimate part of the input.

Definition 4. *A* comprehensive knowledge assertion *has form*

$$\bigwedge \mathcal{CS} \to t{:}F \ ,$$

where $\mathcal{CS}$ *is a finite injective constant specification that specifies all the constants occurring in* t*.*

Each LP-derivation only uses the axiom necessitation rule finitely many times. Hence each derivation of F can be turned into an LP_0-derivation of $\bigwedge \mathcal{CS} \to F$.

Lemma 2. $\mathsf{LP} \vdash t{:}F$ *iff* $\mathsf{LP}_0 \vdash \bigwedge \mathcal{CS} \to t{:}F$ *iff* $\mathsf{rLP}_{\mathcal{CS}} \vdash t{:}F$ *for some finite constant specification* $\mathcal{CS}$*.*

In this section we consider all three proof complexity measures: number of formulas, length, and bit size. In all three cases we show that LP is not logically omniscient. In fact, for the number of lines measure we are able to get a stronger result: LP has polynomial-step proofs of F even in the length of $t{:}F$, i.e., without taking into account constant specifications. For the sake of technical convenience we begin with this result.

5.1 Number of Formulas in the Proof

Throughout this subsection the size of a derivation $\ell(\mathcal{D})$ is the number of formulas in the derivation. Moreover, we allow here arbitrary constant specifications, not necessarily injective.

Theorem 6. LP *is not logically omniscient w.r.t. the Hilbert proof system with the size of a proof being the number of formulas in it.*

Proof. We show that for each valid knowledge assertion $t:F$ there is a Hilbert-style derivation of F which makes a linear number of steps. We will show that actually $3|t|+2$ steps is enough (by $|t|$ we here mean the number of symbols in t).

Indeed, since $\mathsf{LP} \vdash t:F$, by Theorem 5 we have $\mathsf{rLP} \vdash t:F$. It can be easily seen that a derivation of any formula $t:F$ in rLP requires at most $|t|$ steps since each rule increases the size of the outer term by at least 1.

Each axiom of rLP is an instance of an axiom necessitation rule of LP. Each rule of rLP can be emulated in LP by writing the corresponding axiom (LP1 for the $\cdot$-rule, LP2 for the !-rule, or LP3 for the $+$-rule) and using modus ponens once for the latter two cases or twice for the former case. Thus each step of the rLP-derivation is translated as two or three steps of the corresponding LP-derivation. Finally, to derive F from $t:F$ we need to add two formulas: LP4-axiom $t:F \to F$ and formula F by modus ponens. Hence we need at most $3|t|+2$ steps in this Hilbert-style derivation of F. □

The lower bound on the number of steps in the derivation is also encoded by evidence terms. But here we cannot take an arbitrary term t such that $\mathsf{LP} \vdash t:F$. If evidence t corresponds to a very inefficient way of showing validity of F, it would be possible to significantly shorten it. But an efficient evidence term t does give a lower bound on the derivation of F.

Theorem 7. *Let t be the smallest (in dag-size) term such that $\mathsf{LP} \vdash t:F$. Let $\mathcal{D}$ be the shortest Hilbert-style proof of F. Then the number of steps in $\mathcal{D}$ is at least half the number of subterms in t, which is the size of the syntactic dag for t, hence we will denote it by $\dagger(t)$:*

$$\ell(\mathcal{D}) \geq \frac{1}{2}\dagger(t) \ .$$

To give a flavor of the inefficiencies that can be found in t we will prove the following

Lemma 3. *Let t be the smallest*[2] *evidence term such that $\mathsf{LP} \vdash t:F$. Then $+$ does not occur in t.*

Proof. Proof by contradiction. Suppose t is the smallest term such that $\mathsf{LP} \vdash t:F$ and t contains $+$ in it. By Theorem 5, $\mathsf{rLP} \vdash t:F$. Consider an rLP-derivation $\mathcal{R}$

[2] It does not matter whether dag-size or tree-size is considered.

of $t:F$. Any rLP-derivation starts by assigning certain LP-axioms to (occurrences of) evidence constants in t. Then formulas are assigned to more complex subterms of t by induction on the size of the subterm. Consider subterm $s_1 + s_2$. The rule used to assign a formula to this subterm must have form

$$\frac{s_i:G}{(s_1+s_2):G}$$

for some formula G and $i = 1, 2$. If this rule is eliminated from the derivation and the related occurrences of $s_1 + s_2$ in the sibling nodes of the derivation dag are replaced by s_i, we will obtain an rLP-derivation of $t':F$ where t' is the result of replacing several occurrences of s_1+s_2 in t by s_i. It is obvious that $|t'| < |t|$ and $\dagger(t') \leq \dagger(t)$. It may not be that $\dagger(t') < \dagger(t)$ though, e.g. if there were unrelated occurrences of $s_1 + s_2$ in t. But this $+$-elimination procedure can be applied repeatedly until no occurrences of $s_1 + s_2$ are left. After this the dag-size will also decrease. Contradiction. Therefore, t does not contain $+$. □

Proof (of Theorem 7). Let $\mathcal{D}$ be a derivation of F, minimal in the number of steps $N = \ell(\mathcal{D})$. By Lifting Lemma 1, there exists a $+$-free ground term t' such that $\mathsf{LP} \vdash t' : F$. The structure of the derivation tree of $\mathcal{D}$ is almost identical to that of the syntactic tree of t' . The only difference is due to the fact that an axiom necessitation rule $c : A$ in a leaf of a derivation tree corresponds to two nodes in the syntactic tree: for c and for $!c$. But we are interested in the dag sizes of both. Dag structures may have further differences if one evidence constant was used in $\mathcal{D}$ for several axiom necessitation instances. This would further decrease the size of the dag for t'. Hence, for the dag-smallest term t we have

$$\ell(\mathcal{D}) \geq \frac{1}{2}\dagger(t') \geq \frac{1}{2}\dagger(t) \ .$$

□

Combining the results of Theorems 6 and 7 we obtain the following

Corollary 1. *Let t be the dag-smallest term such that $\mathsf{LP} \vdash t:F$. Let $\mathcal{D}$ be the shortest Hilbert-style proof of F. Then*

$$\frac{1}{2}\dagger(t) \leq \ell(\mathcal{D}) \leq 3|t| + 2 \ .$$

Remark 1. Although we were able to obtain both the lower and the upper bound on the size of the derivation, these bounds are not tight, as the tree-size (number of symbols) and the dag-size (number of subterms) can differ exponentially.

Proof. There exists a sequence $\{t_n\}$ of terms such that $|t_n| = 2^{\dagger(t_n)} - 1$. An example of such a sequence is $t_1 = c$, $t_{n+1} = t_n \cdot t_n$.

5.2 Length and Bit Size of Proofs

Let now $\ell(\mathcal{D})$ stand for either the number of symbols in $\mathcal{D}$ or the number of bits in $\mathcal{D}$. Accordingly, let $|F| = \ell(F)$. We will also disallow reusing evidence constants as this may only confuse the knowledge agent, i.e., we assume that constant specifications are injective. This does not limit the scope of LP, since the principal Realization Theorem 4 is established in [2, 3] also for injective constant specifications.

Theorem 8. *Let $\bigwedge \mathcal{CS} \to t:F$ be a comprehensive knowledge assertion, valid in LP_0. Then there exist a polynomial P and a Hilbert-style $\mathsf{LP}_{\mathcal{CS}}$-derivation $\mathcal{D}$ of F such that*

$$\ell(\mathcal{D}) \le P\left(\left|\bigwedge \mathcal{CS} \to t:F\right|\right) \ .$$

Proof. Knowledge assertion $\bigwedge \mathcal{CS} \to t : F$ is valid, hence $\mathsf{rLP}_{\mathcal{CS}} \vdash t : F$ by Lemma 2. A derivation in $\mathsf{rLP}_{\mathcal{CS}}$ will again consist of at most $|t|$ steps, only here we know exactly which axioms were used in the leaves because of injectivity of $\mathcal{CS}$.

Each formula in this derivation has form $s : G$ where s is a subterm of t; let us call these G's evidenced formulas. We claim that the size of evidenced formulas, $|G|$, is bounded by $\ell(\mathcal{CS}) + |t|^2$. Indeed, the rules for $+$ do not change the evidenced formula. The rule for $\cdot$ goes from evidenced formulas $A \to B$ and A to evidenced formula B, which is evidently smaller than $A \to B$. The only rule that does increase the size of the evidenced formula is the rule for !: it yields $s:G$ instead of G. Thus the increase is by $|s| \le |t|$ and the number of !-rules is also bounded by $|t|$.

Therefore the $\mathsf{rLP}_{\mathcal{CS}}$-derivation has at most $|t|$ formulas of size at most $\ell(\mathcal{CS})+|t|^2+|t|$ each. It is clear that the size of the whole derivation is polynomial in $|\bigwedge \mathcal{CS} \to t:F|$.

As before, we convert an $\mathsf{rLP}_{\mathcal{CS}}$-derivation into an $\mathsf{LP}_{\mathcal{CS}}$ derivation as described in the proof of Theorem 6. Evidently, the additional LP-axioms and intermediate results of modus ponens for $\cdot$ only yield a polynomial growth of the derivation size.

Finally, we append the $\mathsf{LP}_{\mathcal{CS}}$-derivation with $t:F \to F$ and F. The resulting derivation of F is polynomial in $|\bigwedge \mathcal{CS} \to t:F|$. □

6 Combining Implicit and Evidence-Based Knowledge

In this section we will extend the Logical Omniscience Test to epistemic systems with justifications [4, 5, 7–9] and show that these systems are logically omniscient with respect to the usual implicit knowledge assertions, but remain non logically omniscient with respect to the evidence-based knowledge assertions.

6.1 Logic S4LP

Logic of knowledge with justification S4LP[3] was introduced in [7–9]. Along with the usual epistemic modality KF '*F is known*' this system contains evidence knowledge assertions $t:F$ ('*F is known for a reason t*') represented by an LP-style module.

The language of S4LP contains both KF and $t:F$ constructs for the same set of evidence terms as in LP. The axioms and rules of S4LP are as follows:

1. finitely many propositional axiom schemes and modus ponens rule,
2. standard S4-axioms with necessitation rule for modality K,
3. axioms LP1–LP4 with the axiom necessitation rule,
4. **Connecting principle** $t:F \to KF$.

S4LP was shown in [7, 19] to be sound and complete with respect to F-models, where modality is given the standard Kripke semantics.

There are two kinds of knowledge assertions in S4LP: implicit KF and evidence-based $t:F$.

Theorem 9. *Implicit knowledge in* S4LP *is logically omniscient (modulo non-collapsing of the polynomial hierarchy), whereas evidence-based knowledge is not.*

Proof. 1. *Implicit knowledge is logically omniscient* in the same sense as S4 was shown to be in Theorems 1 and 2. Logic S4LP was shown to be PSPACE-complete in [30]. It is quite evident that $\mathsf{S4LP} \vdash F$ iff $\mathsf{S4LP} \vdash KF$. Hence the proof of Theorem 1 remains intact for S4LP. Thus implicit knowledge in S4LP is logically omniscient w.r.t. an arbitrary proof system under the bit size measure.

2. Consider the number of formulas in a Hilbert-style proof as the measure of its size. We show how to adapt the proof of Theorem 2 to S4LP. In addition to axioms, modus ponens and necessitation rules, S4LP-derivation also may have axiom necessitation rules $c:A$. For them we need to guess which of the evidence constants c occurring in KF is introduced and which of the axiom schemes those A's belong to. Also for axioms we may need to use variables over evidence terms and unify over them too. These are all the changes needed for the proof. Thus implicit knowledge in S4LP is logically omniscient w.r.t. the number of formulas in Hilbert proofs.

3. *Evidence-based knowledge is not logically omniscient.* The main tool we used in Theorem 6 was N. Krupski's calculus rLP. So we need to develop a similar tool for S4LP. It turns out that the calculus in the language of S4LP with the same rules as rLP suffices.

Definition 5. *Let* rS4LP *be the logic in the language of* S4LP *with the same set of rules as* rLP *and with the maximal constant specification as the set of axioms.*

Lemma 4. $\mathsf{S4LP} \vdash t:F$ *iff* $\mathsf{rS4LP} \vdash t:F$

[3] It was called LPS4 in [7].

Proof. The original proof from [29] remains almost intact. The 'if' part is trivial. For the 'only if' part it is sufficient to use the minimal evidence function in a single-world F-model instead of one in an M-model as in [29] (see also [30]). □

Now we can take the proof of Theorem 6 word for word replacing everywhere in it LP by S4LP and rLP by rS4LP. Thus explicit knowledge in S4LP is not logically omniscient w.r.t. the number of formulas in Hilbert proofs.

4. Similarly, we can define comprehensive knowledge assertions and prove that S4LP is not logically omniscient w.r.t. comprehensive knowledge assertions and Hilbert proofs measured by the number of symbols or number of bits in the proof along the lines of Theorem 8. □

6.2 Multi-agent case

Logics $\mathsf{S4}_n\mathsf{LP}$ of evidence-based common knowledge were introduced in [4, 5] to model multiple agents that all agree with the same set of explicit reasons. Its language contains n knowledge modalities K_i along with $t : F$ constructs for the same set of evidence terms as in LP. The axioms and rules of $\mathsf{S4}_n\mathsf{LP}$ are as follows:

1. finitely many propositional axiom schemes and modus ponens rule,
2. standard S4-axioms with necessitation rule for each modality K_i,
3. axioms LP1–LP4 with the axiom necessitation rule,
4. **Connecting principle** $t{:}F \to K_iF$ for each modality K_i.

Fitting-style models for $\mathsf{S4}_n\mathsf{LP}$ were introduced in [4, 5]. Let W be a non-empty set of worlds. Let $R, R_1, \ldots, R_n$ be reflexive and transitive binary relations on W with $R \supseteq R_i$, $i = 1, \ldots, n$. Let $\mathcal{E}$ be an evidence function satisfying all the conditions from the definition of F-models, where Monotonicity is formulated with respect to accessibility relation R and constant specification is taken to be the maximal for $\mathsf{S4}_n\mathsf{LP}$. Let V be a valuation in the usual modal sense. An $\mathsf{S4}_n\mathsf{LP}$-model is a tuple $\mathcal{M} = (W, R, R_1, \ldots, R_n, \mathcal{E}, V)$ with forcing relation defined as follows:

1. $\mathcal{M}, w \Vdash P$ iff $V(w, P) = t$ for propositional variables P,
2. boolean connectives are classical,
3. $\mathcal{M}, w \Vdash K_iG$ iff $\mathcal{M}, u \Vdash G$ for all wR_iu.
4. $\mathcal{M}, w \Vdash s{:}G$ iff $G \in \mathcal{E}(w, s)$ and $\mathcal{M}, u \Vdash G$ for all wRu.

As was shown in [4, 5], $\mathsf{S4}_n\mathsf{LP}$ is sound and complete with respect to the models described above.

In $\mathsf{S4}_n\mathsf{LP}$, we also have two kinds of knowledge assertions: implicit K_iF and evidence-based $t{:}F$.

Theorem 10. *Implicit knowledge in* $\mathsf{S4}_n\mathsf{LP}$ *is logically omniscient (modulo non-collapsing of the polynomial hierarchy), whereas evidence-based knowledge is not.*

Proof. The same as in Theorem 9 with minor changes.

7 Conclusions

We introduced the Logical Omniscience Test for epistemic systems on the basis of proof complexity considerations, which were inspired by Cook and Reckhow theory (cf. [12, 44]). This test distinguishes the traditional Hintikka-style epistemic modal systems from evidence-based knowledge system. In a large number of cases we show that all these systems are logically omniscient with respect to the usual (implicit) knowledge represented by modal statements K_iF (*i-th agent knows* F), whereas none of these epistemic systems is logically omniscient with respect to evidence-based knowledge assertions $t{:}F$ (F *is known for a reason* t).

One has to be careful when applying the Logical Omniscience Test. This test cannot be the only device to make a judgement about epistemic quality of a system: one could engineer artificial systems to pass the test by throwing out knowledge assertions from a natural epistemic logic. However, comparing modal epistemic logics with the evidence-based systems is fair since, by the Realization Theorem, every knowledge assertion in the former has a representative in the latter. Hence logics of evidence-based knowledge have rich and representative systems of knowledge assertions, both implicit and explicit.

References

1. N. Alechina and B. Logan. Ascribing beliefs to resource bounded agents. In *Proceedings of the 1st International Joint Conference on Autonomous Agents & Multiagent Systems (AAMAS-2002), Bologna, Italy, July 15–19, 2002*, volume II, pages 881–888. ACM Press, 2002.
2. S. Artemov. Operational modal logic. Technical Report MSI 95-29, Cornell University, 1995.
3. S. Artemov. Explicit provability and constructive semantics. *Bulletin of Symbolic Logic*, 7(1):1–36, 2001.
4. S. Artemov. Evidence-based common knowledge. Technical Report TR-2004018, CUNY Ph.D. Program in Computer Science, 2004. Revised version of 2005.
5. S. Artemov. Justified common knowledge. Theoretical Computer Science, to appear 2006.
6. S. Artemov, E. Kazakov, and D. Shapiro. Epistemic logic with justifications. Technical Report CFIS 99-12, Cornell University, 1999.
7. S. Artemov and E. Nogina. Logic of knowledge with justifications from the provability perspective. Technical Report TR-2004011, CUNY Ph.D. Program in Computer Science, 2004.
8. S. Artemov and E. Nogina. Introducing justification into epistemic logic. *Journal of Logic and Computation*, 15(6):1059–1073, 2005.
9. S. Artemov and E. Nogina. On epistemic logic with justification. In Ron van der Meyden, editor, *Proceedings of the 10th Conference on Theoretical Aspects of Rationality and Knowledge (TARK-2005), Singapore, June 10–12, 2005*, pages 279–294. National University of Singapore, 2005.
10. R. Aumann. Reasoning about knowledge in economics. In J. Halpern, editor, *Proceedings of the 1st Conference on Theoretical Aspects of Reasoning about Knowledge (TARK-1986), Monterey, CA, USA, March 1986*, page 251. Morgan Kaufmann, 1986.

11. L. Bonjour. The coherence theory of empirical knowledge. *Philosophical Studies*, 30:281–312, 1976. Reprinted in *Contemporary Readings in Epistemology*, M.F. Goodman and R.A. Snyder (eds). Prentice Hall, pp. 70–89, 1993.
12. S. Cook and R. Reckhow. On the lengths of proofs in the propositional calculus (preliminary version). In *Conference Record of 6th Annual ACM Symposium on Theory of Computing (STOC-1974), Seattle, WA, USA, April 30–May 2, 1974*, pages 135–148. ACM Press, 1974.
13. J. Corbin and M. Bidoit. A rehabilitation of Robinson's unification algorithm. In R. E. A. Mason, editor, *Proceedings of the IFIP 9th World Computer Congress (IFIP Congress-1983), Paris, France, September 19–23, 1983*, pages 909–914. North-Holland, 1983.
14. J. Elgot-Drapkin, M. Miller, and D. Perlis. Memory, Reason, and Time: The Step-logic approach. In R. Cummins and J. Pollock, editors, *Philosophy and AI: Essays at the Interface*, pages 79–103. MIT Press, 1991.
15. R. Fagin and J. Halpern. Belief, awareness, and limited reasoning: Preliminary report. In *Proceedings of the Ninth International Joint Conference on Artificial Intelligence (IJCAI-85)*, pages 491–501, 1985.
16. R. Fagin and J. Halpern. Belief, awareness, and limited reasoning. *Artificial Intelligence*, 34(1):39–76, 1988.
17. R. Fagin, J. Halpern, and M. Vardi. A nonstandard approach to the logical omniscience problem. *Artificial Intelligence*, 79(2):203–240, 1995.
18. M. Fitting. A semantics for the logic of proofs. Technical Report TR-2003012, CUNY Ph.D. Program in Computer Science, 2003.
19. M. Fitting. Semantics and tableaus for LPS4. Technical Report TR-2004016, CUNY Ph.D. Program in Computer Science, 2004.
20. M. Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132(1):1–25, 2005.
21. E. Gettier. Is Justified True Belief Knowledge? *Analysis*, 23:121–123, 1963.
22. A. Goldman. A causal theory of knowing. *The Journal of Philosophy*, 64:335–372, 1967.
23. J. Halpern and Y. Moses. A guide to modal logics of knowledge and belief. In *Proceedings of the Ninth International Joint Conference on Artificial Intelligence (IJCAI-85)*, pages 480–490, 1985.
24. J. Halpern and Y. Moses. A guide to completeness and complexity for modal logics of knowledge and beliefs. *Journal of Artificial Intelligence*, 54:319–379, 1992.
25. V. Hendricks. Active agents. *Journal of Logic, Language and Information*, 12(4):469–495, 2003.
26. J. Hintikka. *Knowledge and Belief*. Cornell University Press, 1962.
27. J. Hintikka. Impossible possible worlds vindicated. *Journal of Philosophical Logic*, 4:475–484, 1975.
28. K. Konolige. *A Deductive Model of Belief*. Research Notes in Artificial Intelligence. Morgan Kaufmann, 1986.
29. N. Krupski. On the complexity of the reflected logic of proofs. Technical Report TR-2003007, CUNY Ph.D. Program in Computer Science, 2003.
30. R. Kuznets. Complexity of evidence-based knowledge. Accepted for publication in proceeding of Rationality and Knowledge workshop of ESSLLI-2006, 2006.
31. R. Ladner. The computational complexity of provability in systems of modal propositional logic. *SIAM Journal on Computing*, 6(3):467–480, 1977.
32. K. Lehrer and T. Paxson. Knowledge: undefeated justified true belief. *The Journal of Philosophy*, 66:1–22, 1969.

33. W. Lenzen. Knowledge, belief and subjective probability. In V. Hendricks, K. Jörgensen, and S. Pedersen, editors, *Knowledge Contributors*. Kluwer, 2003.
34. H. Levesque. A logic of implicit and explicit belief. In R. Brachman, editor, *Proceedings of the National Conference on Artificial Intelligence (AAAI-1984), Austin, TX, USA, August 6–10, 1984*, pages 198–202. AAAI Press, 1984.
35. D. Lewis. Elusive knowledge. *Australian Journal of Philosophy*, 7:549–567, 1996.
36. A. Mkrtychev. Models for the logic of proofs. In S. Adian and A. Nerode, editors, *Logical Foundations of Computer Science' 97, Yaroslavl'*, volume 1234 of *Lecture Notes in Computer Science*, pages 266–275. Springer, 1997.
37. R. Montague. Universal Grammar. *Theoria*, 36:373–398, 1970.
38. R. Moore. Reasoning about knowledge in artificial intelligence. In J.Y. Halpern, editor, *Proceedings of the 1st Conference on Theoretical Aspects of Reasoning about Knowledge (TARK-1986), Monterey, CA, USA, March 1986*, page 81. Morgan Kaufmann, 1986.
39. Y. Moses. Resource-bounded knowledge. In M. Vardi, editor, *Proceedings of the 2nd Conference on Theoretical Aspects of Reasoning about Knowledge (TARK-1988), Pacific Grove, CA, USA, March 1988*, pages 261–275. Morgan Kaufmann, 1988.
40. R. Nozick. *Philosophical Explanations*. Harvard University Press, 1981.
41. R. Parikh. Knowledge and the problem of logical omniscience. In Z. Ras and M. Zemankova, editors, *Proceedings of the 2nd International Symposium on Methodologies for Intelligent Systems (ISMIS-1987), Charlotte, NC, USA, October 14–17, 1987*, pages 432–439. North-Holland, 1987.
42. R. Parikh. Logical omniscience. In D. Leivant, editor, *Logical and Computational Complexity. Selected Papers. Logic and Computational Complexity, International Workshop (LCC-1994), Indianapolis, IN, USA, October 13–16, 1994*, volume 960 of *Lecture Notes in Computer Science*, pages 22–29. Springer, 1995.
43. R. Parikh. Logical omniscience and common knowledge: WHAT do we know and what do WE know? In R. van der Meyden, editor, *Proceedings of the 10th Conference on Theoretical Aspects of Rationality and Knowledge (TARK-2005), Singapore, June 10–12, 2005*, pages 62–77. National University of Singapore, 2005.
44. P. Pudlak. The Lengths of Proofs. In S. Buss, editor, *Handbook of Proof Theory*, pages 547–637. Elsevier, 1998.
45. V. Rantala. Impossible worlds semantics and logical omniscience. *Acta Philosophica Fennica*, 35:18–24, 1982.
46. D. Scott. Advice in modal logic. In K. Lambert, editor, *Philosophical Problems in Logic*, pages 143–173. Reidel, 1970.
47. M. Vardi. On epistemic logic and logical omniscience. In J. Halpern, editor, *Proceedings of the 1st Conference on Theoretical Aspects of Reasoning about Knowledge (TARK-1986), Monterey, CA, USA, March 1986*, pages 293–305. Morgan Kaufmann, 1986.
48. H. Wansing. A general possible worlds framework for reasoning about knowledge. *Studia Logica*, 49(4):523–539, 1990.