2010

TR-2010014: A Complexity Question in Justification Logic

Antonis Achilleos

A Complexity Question in Justification Logic

Antonis Achilleos

December 12, 2010

Abstract

Bounds for the computational complexity of major justification logics were found in papers by Buss, N. Krupski, Kuznets, and Milnikel: logics J, J4, JT, LP and JD, were established to be Σ_2^p-complete. A corresponding lower bound is also known for JD4, the system that includes the consistency axiom and positive introspection. However, no upper bound has been established so far for this logic. Here, the missing upper bound for the complexity of JD4 is established through an alternating algorithm. It is shown that using Fitting models of only two worlds is adequate to describe JD4; this helps to produce an effective tableau procedure and essentially is what distinguishes the new algorithm from existing ones.

1 Introduction

The classical analysis of knowledge includes the notion of justification, e.g., the famous tripartate view of knowledge as justified, true belief, usually attributed to Plato. Hintikka's modal logic approach represents knowledge as true belief. Justification logic extends epistemic logic by supplying the missing third component of Plato's characterization.

The Logic of Proofs LP was the first justification logic to be introduced, by Artemov, in [1, 2] (see also [3]). Later, variations appeared in [5] corresponding to well-known normal modal logics. Two types of semantics are known for justification logics: M-models, introduced by Mkrtychev ([12, 17]) and F-models, introduced by Fitting ([4, 8, 9, 14, 18]). F-models resemble Kripke models for normal modal logics equipped with an additional mechanism, the admissible evidence function, usually represented by $\mathcal{A}$. For a term t and formula ϕ, $\mathcal{A}(t, \phi)$ will be the set of worlds in the model where t is appropriate evidence for ϕ. $t:\phi$ is true in a world iff ϕ is true in every accessible world and the world in question is in $\mathcal{A}(t, \phi)$. M-models are essentially F-models of only one world. In this setting $\mathcal{A}(t, \phi)$ will be either *true* or *false*.

Upper and lower bounds are known for the computational complexity of justification logics J, J4, JT, LP and JD, and determine them to be Σ_2^p -complete ([6, 10, 12, 13, 15, 16]). In [15], Kuznets presents a new algorithm for checking JD-satisfiability. This algorithm is in many perspectives similar to the ones for other justification mentioned here: J, J4, JT, LP. A tableau method is used to non-deterministically construct a model that satisfies the formula in question, then the algorithm checks whether the produced conditions for the admissible evidence function are legitimate. This last check is known to be in NP ([10, 13]) and is, in fact, NP-complete ([7]). Therefore, the resulting overall algorithm is a polynomial time alternating algorithm with one alternation, starting from a universal state and eventually reaching an existential state[1], which establishes that the problem is in Π_2^p and therefore the logic is in Σ_2^p.

The difference among the cases that have been dealt with previously lies in the consistent evidence property of logics JD and JD4 (the "D"); in an M-model of these logics, we can never have $\mathcal{A}(t, \perp)$. In other words, if $t_1 : \phi_1, \ldots, t_n : \phi_n$ are satisfied in a model, the set $\{\phi_1, \ldots, \phi_n\}$ must be consistent. To incorporate this condition, the algorithm continues and tries to verify whether this set, $\{\phi_1, \ldots, \phi_n\}$, is satisfiable in another model with another tableau construction. This is done by utilizing additional numerical prefixes on the prefixed formulas. A sequence of models is thus produced.

Although this construction, like all previous ones, is based on the compact character of M-models for justification logics, it produces something that resembles something very similar to an F-model. In general, when discussing complexity issues for justification logics, working with F-models appears inconvenient and unnecessary: many possible worlds could succeed a current world. Furthermore, the admissible evidence function is defined on this multitude of worlds, making it virtually prohibitive to use this setting to discuss complexity issues. On the other hand, M-models consist of only one world. The admissible evidence function is by far less complicated and the conditions it should satisfy can be checked by an NP-algorithm, except in the case of JD and JD4. For these logics, the additional condition that for any justification term t, $\mathcal{A}(t, \perp) = \mathit{false}$ cannot be verified as easily due to the negative nature of this condition. It would be nice to be able to sacrifice some, but not much, of the compact description of M-models for more convenient conditions on $\mathcal{A}$ and indeed, it seems that in the case of JD, this is

[1]Or, this can be viewed as a coNP algorithm using an oracle from NP.

exactly what can be done to provide a solution. Now, this idea will be taken a small step forward to provide a similar Σ_2 algorithm for $\mathsf{JD4}$-satisfiability. Additionally, the positive introspection axiom of $\mathsf{JD4}$ will help provide an even simpler class of models than in the case of JD, making the study of its complexity easier. Specifically, it is discovered that using Fitting-like models of only two worlds is adequate to describe $\mathsf{JD4}$.

2 The logic $\mathsf{JD4}$

$\mathsf{JD4}$ was first introduced in [5] as a variation of LP, the Logic of Proofs. It is the explicit counterpart of D4, both in intuition, as there is some similarity their axioms, and in a more precise way (see [5]).

The language will include justification constants $c_i,\ i \in \mathbb{N}$, justification variables: $x_i,\ i \in \mathbb{N}$ and justification terms, usually denoted $t, s, \ldots$. These are defined as follows.

Definition 1 (Justification Terms)**.**

- *Constants ($c_i,\ i \in \mathbb{N}$) and variables ($x_i,\ i \in \mathbb{N}$) are terms;*
- *If t_1, t_2 are terms, so are*

$$(t_1 \cdot t_2),\ (t_1 + t_2),\ (!t_1).$$

"$\cdot$" is usually called application, "+" is called sum, and "!" proof checker. The set of justification terms will be called Tm.

Also, propositional variables will be used in the language: $p_i,\ i \in \mathbb{N}$. The set of propositional variables will be called $SLet$. The formulas of the language are

Definition 2 (Justification Formulas)**.**

- *All propositional variables ($p_i,\ i \in \mathbb{N}$) are formulas*
- *If p is a propositional variable, t is a term and ϕ, ψ are formulas, then so are*

$$p,\ \bot,\ (\phi \to \psi),\ (t{:}\phi)$$

$\neg\phi$ can be seen as short for $\phi \to \bot$, and the rest of the connectives can be defined from these in the usual way. Also as usual, parentheses will be omitted using standard conventions, and naturally, $!s : s : \phi$ will be read as $(!s{:}(s{:}\phi))$. Fm will denote the set of justification formulas.

The axioms of $\mathsf{JD4}_\emptyset$ are the following.

A1 Finitely many schemes of classical propositional logic;

A2 $s\!:\!(\phi \to \psi) \to (t\!:\!\phi \to (s \cdot t)\!:\!\psi)$ - Application Axiom;

A3

$$\begin{array}{ll} s\!:\!\phi \to (s+t)\!:\!\phi & \\ s\!:\!\phi \to (t+s)\!:\!\phi & \text{- Monotonicity Axiom;} \end{array}$$

A5 $t\!:\!\phi \to !t\!:\!t\!:\!\phi$ - Positive introspection;

A6 $t\!:\!\bot \to \bot$ - Consistency Axiom
and Modus Ponens.

MP Modus Ponens Rule :

$$\frac{\phi \to \psi \qquad \phi}{\psi}\ .$$

Definition 3. *A constant specification for a justification logic JL is any set*

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

A c.s. is axiomatically appropriate *if each axiom is justified by at least one constant,* schematic *if every constant justifies a certain number of axiom schemes (0 or more), and* schematically injective *if it is schematic and every constant justifies at most one scheme.*

Definition 4. *Given a constant specification* $\mathcal{CS}$ *for* JD4*, the logic* $\mathsf{JD4}_{\mathcal{CS}}$ *is* $\mathsf{JD4}_{\emptyset}$*, with the additional rule*

$$\frac{}{c\!:\!A}\ \mathrm{R4}_{\mathcal{CS}}$$

where $c\!:\!A \in \mathcal{CS}$*.*

A definition of the (Fitting) semantics for $\mathsf{JD4}_{\mathcal{CS}}$ follows.

Definition 5 ([4, 8, 9, 14, 18])**.** *An F-model* $\mathcal{M}$ *for* $\mathsf{JD4}_{\mathcal{CS}}$ *is a quadruple* $(W, R, V, \mathcal{A})$*, where* $W \neq \emptyset$ *is the set of worlds (or states) of the model,* R *is a transitive and serial (for any* $a \in W$ *there is some* $b \in W$ *such that* aRb*) binary relation on* W*,* V *assigns a subset of* W *to each propositional variable,* p*, and* $\mathcal{A}$ *assigns a subset of* W *to each pair of a justification term and a formula. Additionally,* $\mathcal{A}$ *must satisfy the following conditions:*

- *Application closure: for any formulas* ϕ, ψ *and justification terms* t, s*,*

$$\mathcal{A}(s, \phi \to \psi) \cap \mathcal{A}(t, \phi) \subseteq \mathcal{A}(s \cdot t, \psi).$$

- *Sum closure: for any formula* ϕ *and justification terms* t, s,

$$\mathcal{A}(t,\phi) \cup \mathcal{A}(s,\phi) \subseteq \mathcal{A}(t+s,\phi).$$

- *Simplified* $\mathcal{CS}$*-closure: for any axiom* A*, constant* c*, such that* $c\!:\!A \in \mathcal{CS}$,

$$\mathcal{A}(c,A) = W.$$

- *Positive introspection closure: for any formula* ϕ *and justification term* t,

$$\mathcal{A}(t,\phi) \subseteq \mathcal{A}(!t, t\!:\!\phi).$$

- *Monotonicity: for any formula* ϕ*, justification term* t *and* $a, b \in W$*, if* aRb *and* $a \in \mathcal{A}(t,\phi)$*, then* $b \in \mathcal{A}(t,\phi)$.

Truth in the model is defined in the following way, given a state a*:*

- $M, a \not\models \bot$.
- *If* p *is a propositional variable, then* $\mathcal{M}, a \models p$ *iff* $a \in V(p)$
- *If* ϕ, ψ *are formulas, then* $\mathcal{M}, a \models \phi \to \psi$ *if and only if* $M, a \models \psi$*, or* $\mathcal{M}, a \not\models \phi$.
- *If* ϕ *is a formula and* t *a term, then* $\mathcal{M}, a \models t:\phi$ *if and only if* $a \in \mathcal{A}(t,\phi)$ *and for all* $b \in W$*, if* aRb*, then* $\mathcal{M}, b \models \phi$.

$\mathsf{JD4}_{\mathcal{CS}}$ *is sound and complete w.r.t. its F-models, for an axiomatically appropriate constant specification. Additionally, it is complete w.r.t. its F-models that satisfy the following property.*

Strong Evidence Property: $\mathcal{M}, a \models t\!:\!\phi$ *if and only if* $a \in \mathcal{A}(t,\phi)$.

It is also useful to present Mkrtychev (M-) models for $\mathsf{JD4}$. M-models are F-models with just one world. However, since if we insisted on seriality, we would introduce factivity ($t\!:\!\phi \to \phi$ would be valid), this condition is replaced by another, the *consistent evidence condition* (in the definition below).

Definition 6 ([12, 17])**.** *An* M-model for $\mathsf{JD4}_{\mathcal{CS}}$*, where* $\mathcal{CS}$ *is a constant specification for* $\mathsf{JD4}$ *is a pair*

$$\mathcal{M} = (V, \mathcal{A}),$$

where propositional valuation

$$V : SLet \longrightarrow \{\mathit{true}, \mathit{false}\}$$

assigns a truth value to each propositional variable and

$$\mathcal{A} : Tm \times Fm \longrightarrow \{true, false\}$$

is an admissible evidence function*.* $\mathcal{A}(t,\phi)$ *will be used as an abbreviation for* $\mathcal{A}(t,\phi) = true$ *and* $\neg\mathcal{A}(t,\phi)$ *as an abbreviation for* $\mathcal{A}(t,\phi) = false$.
The admissible evidence function must satisfy certain closure conditions:

Application Closure: *If* $\mathcal{A}(s, \phi \to \psi)$ *and* $\mathcal{A}(t,\phi)$ *then* $\mathcal{A}(s \cdot t, \psi)$.

Sum Closure: *If* $\mathcal{A}(s,\phi)$ *then* $\mathcal{A}(s+t,\phi)$.
If $\mathcal{A}(t,\phi)$ *then* $\mathcal{A}(s+t,\phi)$.

Simplified $\mathcal{CS}$ Closure: *If* $c{:}A \in \mathcal{CS}$, *then* $\mathcal{A}(c, A)$.

Positive Introspection Closure *If* $\mathcal{A}(t,\phi)$ *then* $\mathcal{A}(!t, t{:}\phi)$

Consistent Evidence Condition $\mathcal{A}(t,\bot) = false$,

for any formulas ϕ, ψ, *any terms* s, t, *any* $c{:}A \in \mathcal{CS}$, *and any integer* $n \geq 1$.
The truth relation $\mathcal{M} \models H$ *is defined as follows:*

- $\mathcal{M} \models p$ *iff* $V(p) = true$
- $\mathcal{M} \not\models \bot$
- $\mathcal{M} \models \phi \to \psi$ *iff* $\mathcal{M} \not\models \phi$ *or* $\mathcal{M} \models \psi$
- $\mathcal{M} \models t{:}\phi$ *iff* $\mathcal{A}(t,\phi)$

for any formulas ϕ, ψ, *any term* t *and any propositional variable* p.
$\mathsf{JD4}_{\mathcal{CS}}$ *is sound and complete with respect to its M-models.*

The following definition will prove useful later on.

Definition 7. *Given an F-model* $\mathcal{M}$, *a world* w *of the model and a formula* $t{:}\phi$, *we say that* $t{:}\phi$ *is* factive *at world* w *of* $\mathcal{M}$, *if and only if* $\mathcal{M}, w \models t{:}\phi \longrightarrow \phi$. *Similarly, we can define when* $t{:}\phi$ *is factive in an M-model. A set* Φ *of formulas of the form* $t{:}\phi$ *will be factive exactly when all elements of* Φ *are factive.*

3 $*$-calculus and minimal evidence functions

In this section, the $*$-calculus is defined. The $*$-calculus provides an independent axiomatization of the reflected fragments of justification logics and is an invaluable tool in the study of the complexity of these logics. The concepts, notation and results in this section come from [11, 13, 17].

Definition 8 (Star-expressions)**.** *If t is a term and ϕ is a formula, then $*(t,\phi)$ is a star-expression ($*$-expression).*

Definition 9. *For any justification logic L and constant specification $\mathcal{CS}$, the reflected fragment of $L_{\mathcal{CS}}$ is*

$$rL_{\mathcal{CS}} = \{t\!:\!\phi \mid L_{\mathcal{CS}} \vdash t\!:\!\phi\}.$$

Definition 10 ($*$-calculus)**.** *$*\mathcal{CS}$ Axioms: $*(c, A)$, where $c\!:\!A \in \mathcal{CS}$.*

$*A2$

$$\frac{*(s, \phi \rightarrow \psi) \qquad *(t,\phi)}{*(s \cdot t, \psi)}$$

$*A3$

$$\frac{*(t,\phi)}{*(s+t,\phi)} \qquad \frac{*(s,\phi)}{*(s+t,\phi)}$$

$*A4$

$$\frac{*(t,\phi)}{*(!t, t\!:\!\phi)}$$

The calculus: *The $*!_{\mathcal{CS}}$-calculus is a calculus on starred expressions and includes $*\mathcal{CS}, A2, A3$ and $A4$.*

Theorem 1 ([10, 13])**.** *For any constant specification $\mathcal{CS}$,*

$$\mathsf{rJD4}_{\mathcal{CS}} \vdash t\!:\!\phi \iff \mathsf{rJD4}_{\mathcal{CS}} \vdash t\!:\!\phi \iff \vdash_{*!_{\mathcal{CS}}} *(t,\phi).$$

Possible evidence functions are presented next, together with a way to produce a minimal evidence function for an M-model.

Definition 11. *An M-type possible evidence function is any function*

$$\mathcal{B} : Tm \times Fm \longrightarrow \{true, false\}.$$

A possible evidence function is essentially an admissible evidence function with no conditions imposed on it.

Definition 12. *We say that an M-type possible evidence function $\mathcal{B}_2$ is based on an M-type possible evidence function $\mathcal{B}_1$ and write*

$$\mathcal{B}_1 \subseteq \mathcal{B}_2,$$

if for all terms t and formulas ϕ,

$$\mathcal{B}_1(t, \phi) \Longrightarrow \mathcal{B}_2(t, \phi).$$

Definition 13. *Let $\mathcal{EF}$ be a class of M-type possible evidence functions. A possible evidence function $\mathcal{B} \in \mathcal{EF}$ is called the minimal evidence function in $\mathcal{EF}$ if for all $\mathcal{B}' \in \mathcal{EF}$,*

$$\mathcal{B} \subseteq \mathcal{B}'.$$

Definition 14. *For some possible evidence function $\mathcal{B}$, $\mathcal{B}^* = \{*(t, \phi) | \mathcal{B}(t, \phi) = true\}$.*

Theorem 2 ([17])**.** *For any $\mathcal{CS}$ constant specification for $\mathsf{JD4}$ and any possible evidence function $\mathcal{B}$, the class of M-type admissible evidence functions for $\mathsf{JD4}_{\mathcal{CS}}$ based on $\mathcal{B}$ is symbolized $\mathcal{AEF}_{\mathcal{B}}(\mathsf{JD4}_{\mathcal{CS}})$, and if nonempty has a unique minimal element $\mathcal{A}$, which is the following:*

$$\mathcal{A}(t, \phi) \Longleftrightarrow \mathcal{B}^* \vdash_{*!_{\mathcal{CS}}} *(t, \phi).$$

Note. In the following, an F-type admissible evidence function when considering a single world of the model may be treated as an M-type admissible evidence function, when the appropriate conditions are met. Despite changes in notation, under certain circumstances this is entirely acceptable and in fact this change in perspective will be very useful and frequent. Finally, it is useful, given an F-type admissible evidence function $\mathcal{A}$ and a world u, to define $\mathcal{A}_u$ to be the set $\{(t, \phi) | u \in \mathcal{A}(t, \phi)\}$.

Finally, since we are discussing complexity issues, it is natural that the following theorem is relevant. In fact, it will prove to be extremely useful later on.

Theorem 3 ([10, 13])**.** *Let $\mathcal{CS}$ be a schematic constant specification decidable in polynomial time. Then, there exists a non-deterministic algorithm that runs in polynomial time and determines, given a finite set S of $*$-expressions, a formula ϕ and a term t, whether*

$$S \vdash_{*!_{\mathcal{CS}}} *(t, \phi).$$

4 A class of models

In the following, the constant specification $\mathcal{CS}$ will be assumed to be axiomatically appropriate and, when discussing complexity issues, efficiently decidable. The algorithm that will be presented and its correctness will be based on the following proposition.

Proposition 4. *A formula ϕ is $\mathsf{JD4}_{\mathcal{CS}}$-satisfiable if and only if it is satisfiable by an F-model $\mathcal{M} = (W, R, V, \mathcal{A})$ for $\mathsf{JD4}_{\mathcal{CS}}$ that additionally has the following properties:*

- *W has exactly two elements, a, b.*
- *$R = \{(a, b), (b, b)\}$.*

Proof. Let ϕ be a formula that is $\mathsf{JD4}_{\mathcal{CS}}$-satisfiable and let $\mathcal{M}^* = (W, R, V, \mathcal{A})$ be a model and $a \in W$ a world of the model that satisfies ϕ. Assume that $\mathcal{M}^*$ satisfies the Strong Evidence Property.

We know that R is serial and transitive and that $\mathcal{A}$ satisfies the monotonicity property. From this, we know that there is an infinite sequence of elements of W, $\alpha = (a_i)_{i \in \mathbb{N}}$, such that $a_0 = a$, $i < j \Rightarrow a_i R a_j$ & $\mathcal{A}_{a_i} \subseteq \mathcal{A}_{a_j}$.

For any $t{:}F$, there is at most one $j \in \mathbb{N}$, $\mathcal{M}^*, a_j \not\models t{:}F \to F$. Otherwise, there are $i < j$ s.t. $\mathcal{M}^*, a_i, a_j \not\models t{:}F \to F$. Since $\mathcal{M}^*, a_i \not\models t{:}F \to F$, we have $\mathcal{M}^*, a_i \models t{:}F$. From this, it follows that $\mathcal{M}^*, a_j \models F$, so $\mathcal{M}^*, a_j \models t{:}F \to F$ - a contradiction.

Therefore, for any set of term-prefixed formulas, there is an i, after which all terms of α are factive with respect to that set. More specifically, let Φ be the set of term-prefixed subformulas of ϕ and let b be a term of α, where Φ is factive.

Define $\mathcal{M}$ to be the model $(\{a, b\}, \{(a, b), (b, b)\}, V', \mathcal{A}')$, such that $V', \mathcal{A}'$ agree with $V, \mathcal{A}$ on a, b. That is, for any $w \in \{a, b\}$, t term, ψ formula, p propositional variable, $w \in V(p)$ if and only if $w \in V'(p)$, and $w \in \mathcal{A}(t, \psi)$ if and only if $w \in \mathcal{A}'(t, \psi)$. It is easy to see that the new model satisfies the conditions required of F-models for $\mathsf{JD4}_{\mathcal{CS}}$[2].

By induction on the structure of χ, we can show that for any χ, subformula of ϕ, $\mathcal{M}^*, b \models \chi$ iff $\mathcal{M}, b \models \chi$ (and the propositional cases are trivial, so). If $\chi = t : \omega$, then $\mathcal{M}^*, b \models \chi$ iff $\mathcal{M}^*, b \models t : \omega$ iff $\mathcal{M}^*, b \models \omega$ and $b \in \mathcal{A}(t, \omega)$ (Strong Evidence) iff $\mathcal{M}, b \models \omega$ and $b \in \mathcal{A}'(t, \omega)$ iff $\mathcal{M}, b \models \chi$.

[2] Of course, we assume here that $a \neq b$, but this is a legitimate assumption. If we need to make this explicit, we could simply have $W = \{(a, 0), (b, 1)\}$ and the accessibility relation, V', A' behave in the same way.

To prove that $\mathcal{M}, a \models \phi$, we will first prove that

$$\mathcal{M}^*, a \models \psi \Leftrightarrow \mathcal{M}, a \models \psi,$$

for any ψ subformula of ϕ, by induction on the structure of ψ. If ψ is a propositional variable, and for the propositional cases, again, this is obvious and the only interesting case is when $\psi = t\!:\!\chi$. In this case, $\mathcal{M}^*, a \models t\!:\!\chi$ iff $a \in \mathcal{A}(t, \chi)$ and $M^*, b \models \chi$ iff $a \in \mathcal{A}'(t, \chi)$ and $M, b \models \chi$ iff $\mathcal{M}, a \models t\!:\!\chi$. $\square$

Observation 1. Note that we can now replace the admissible evidence function with another, say $\mathcal{A}^m$, such that $w \in \mathcal{A}^m(t, \psi)$ iff $\mathcal{M}, w \models t\!:\!\psi$. This new function will satisfy the necessary conditions to be an admissible evidence function and the new model will satisfy the same formulas as the old one in the same worlds. Therefore, we can claim the following corollary.

Corollary 5. *A formula is* $\mathsf{JD4}_{\mathcal{CS}}$*-satisfiable if and only if it is satisfiable by an F-model* $\mathcal{M} = (W, R, V, \mathcal{A})$ *for* $\mathsf{JD4}_{\mathcal{CS}}$ *that additionally has the following properties:*

- W *has exactly two elements,* a, b*;*
- $R = \{(a, b), (b, b)\}$*;*
- $a \in \mathcal{A}(t, F)$ *if and only if* $\mathcal{M}, a \models t\!:\!F$ *for all* $t\!:\!F$*. (Strong Evidence Condition)*

5 The algorithm and its analysis

Neither the algorithm that determines $\mathsf{JD4}_{\mathcal{CS}}$-satisfiability nor its analysis is particularly novel (c.f. [12, 13, 15]). It is in fact based on the ones already used to establish the same upper bound for the satisfiability for J, J4, JT, LP, except for certain differences that stem from the fact that we are discussing a different logic and thus the algorithm is based on a different class of models. It is based on a tableau construction.

Prefixed expressions will be used and there will be two types of prefixes and two types of expressions. The first will be the usual T or F prefix and the other will be the prefix that will intuitively denote the world we are referring to; these are a and b. So, the prefixed formulas will be of the form $w\ P\ e$, where $w \in \{a, b\}, P \in \{T, F\}$ and e is either a formula of the language or a $*$-expression. w will be called the world prefix and P the truth prefix.

As was mentioned previously, the algorithm will be based on a tableau construction. The propositional tableau rules will be the ones usually used and they are not mentioned here. The non-propositional cases are covered by the following rules.

$$\frac{a\ T\ s{:}\psi}{\begin{array}{c}a\ T\ *(s,\psi)\\ b\ T\ s{:}\psi\end{array}}, \qquad \frac{b\ T\ s{:}\psi}{\begin{array}{c}b\ T\ *(s,\psi)\\ b\ T\ \psi\end{array}},$$

$$\frac{a\ F\ s{:}\psi}{a\ F\ *(s,\psi) \mid a\ F\ \psi}, \qquad \frac{b\ F\ s{:}\psi}{b\ F\ *(s,\psi) \mid b\ F\ \psi}$$

The algorithm runs in two phases.

During the first phase, the algorithm will construct a tableau branch using the tableau rules in a non-deterministic way. After all possible tableau derivations have been applied, there are two possibilities for the constructed branch. It can either be propositionally closed, that is, it could contain $w\ T\ e$ and $w\ F\ e$, or it can be complete, that is, the branch is not propositionally closed and no application of a tableau rule gives a new prefixed formula. If it is propositionally closed, the input is rejected, otherwise, the second phase of the algorithm begins. Let X_a be the set of star expressions prefixed with $a\ T$ and X_b the set of star expressions prefixed with $b\ T$ in the branch. Confirm that no expression of the form $*(t,\phi)$ that appears negatively in the branch for world prefix w can be derived from X_w. If this is indeed the case, the algorithm accepts, otherwise, it rejects.

The proof of the correctness of the algorithm follows.

Proof. Supposing formula ϕ is satisfiable by $\mathcal{M} = (\{a,b\},\{(a,b),(b,b)\},V,\mathcal{A})$ such as the ones described above and starting the procedure with $a\ T\ \phi$, it is easy to see that there is a way to perform the tableau rules while producing a-prefixed expressions satisfied at world a and b-prefixed expressions satisfied at world b. Now, if X_w derives $*(t,\psi)$, then the minimal evidence function that includes X_w should also include (t,ψ) (by Theorem 2), and therefore so should $\mathcal{A}$ in the corresponding world. Therefore, no such negative expression will be derivable by X_w. In conclusion, the algorithm accepts.

On the other hand, suppose the algorithm accepts. Suppose a complete branch of the tableau that is produced in an accepting branch of the computation tree. A model will be constructed to satisfy ϕ. This will be $\mathcal{M} = (\{a,b\},\{(a,b),(b,b)\},V,\mathcal{A})$. $V(p)$ will include a iff $a\ T\ p$ appears in the tableau and similarly for b. $\mathcal{A}$ on a will be the minimal evidence function that includes (t,ψ) iff $a\ T\ *(t,\psi)$ appears in the tableau and again, similarly for b. Since by the tableau rules, $X_a \subseteq X_b$, monotonicity is satisfied. If $\mathcal{A}$ so defined includes any negative $*$-expression in any of the two worlds, the second step of the algorithm would have rejected the input and the computation branch would not be accepting (again, by Theorem 2).

The model satisfies at a all a-prefixed expressions and at world b all b-prefixed expressions. This can be proven by induction on the structure of the expressions. By the above argument, this is automatically true for starred expressions. Also, by definition of V, this is true for propositional variables. Propositional cases are easy, so it remains to show this for formulas of the form $t{:}\psi$.

First, for b-prefixed formulas. If $b\ T\ t{:}\psi$ is in the branch, there must also be $b\ T\ *(t,\psi)$ and $b\ T\ \psi$. By I.H., these are already satisfied, so $b \in \mathcal{A}(t,\psi)$ and $\mathcal{M}, b \models \psi$. Therefore, $\mathcal{M}, b \models t:\psi$. If $b\ F\ t:\psi$ is in the branch, then the branch must also include either $b\ F\ \psi$ or $b\ F\ *(t,\psi)$. In either case, the conclusion is $\mathcal{M}, b \not\models t{:}\psi$.

Finally, the case of a-prefixed formulas. If $a\ T\ t{:}\psi$ is in the branch, there must also be $a\ T\ *(t,\psi)$ and $b\ T\ \psi$ (and $b\ T\ t{:}\psi$ too, but it is not relevant here). By I.H., these are already satisfied, so $a \in \mathcal{A}(t,\psi)$ and $\mathcal{M}, b \models \psi$. Therefore, $\mathcal{M}, a \models t:\psi$. If $a\ F\ t:\psi$ is in the branch, then the branch must also include either $b\ F\ \psi$ or $a\ F\ *(t,\psi)$. In either case, the conclusion is $\mathcal{M}, b \not\models t{:}\psi$.

This completes the correctness proof of the algorithm. □

The first phase of the algorithm runs in nondeterministic polynomial time, while the second checks a condition known to be in coNP (Theorem 3). Therefore, the algorithm establishes that JD4-satisfiability is in Σ_2^p. The following corollary follows immediately.

Corollary 6. *$\mathsf{JD4}_{\mathcal{CS}}$ is in Π_2^p for any axiomatically appropriate, schematic, and efficiently decidable $\mathcal{CS}$.*

The following has been recently proven in [6].

Theorem 7 ([6])**.** *$\mathsf{JD4}_{\mathcal{CS}}$ is Π_2^p-hard, for any axiomatically appropriate, and schematically injective $\mathcal{CS}$.*

Finally, combining these two results, we can claim the following.

Corollary 8. *$\mathsf{JD4}_{\mathcal{CS}}$ is Π_2^p-complete, for any axiomatically appropriate, schematically injective, and efficiently decidable $\mathcal{CS}$.*

Aknowledgements

The author would like to thank Sergei Artemov for his encouragement and essential suggestions and Karen Kletter for her invaluable help in editing.

References

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

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

[3] Sergei Artemov. Kolmogorov and Gödel's approach to intuitionistic logic: current developments. *Russian Mathematical Surveys*, 59(2):203–229, 2004. Originally published in Russian.

[4] Sergei Artemov. The logic of justification. *The Review of Symbolic Logic*, 1(4):477–513, 2008.

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

[6] Samuel R. Buss and Roman Kuznets. Lower complexity bounds in justification logic. *Manuscript*, 2009.

[7] Samuel R. Buss and Roman Kuznets. The NP-completeness of reflected fragments of justification logics. In Sergei Artëmov and Anil Nerode, editors, *LFCS*, volume 5407 of *Lecture Notes in Computer Science*, pages 122–136. Springer, 2009.

[8] Melvin Fitting. A semantics for the Logic of Proofs. Technical Report TR–2003012, CUNY Ph.D. Program in Computer Science, 2003.

[9] Melvin Fitting. The logic of proofs, semantically. *Annals of Pure and Applied Logic*, 132(1):1–25, 2005.

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

[11] Vladimir N. Krupski. Referential logic of proofs. *Theoretical Computer Science*, 357(1–3):143–166, 2006.

[12] Roman Kuznets. On the complexity of explicit modal logics. In *Proceedings of the 14th Annual Conference of the EACSL on Computer Science Logic*, pages 371–383, London, UK, 2000. Springer-Verlag.

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

[14] 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.

[15] Roman Kuznets. Complexity through tableaux in justification logic. In *2008 European Summer Meeting of the Association for Symbolic Logic, Logic Colloquium '08, Bern, Switzerland, July 3–July 8, 2008*, volume 15(1) of *Bulletin of Symbolic Logic*, page 121. Association for Symbolic Logic, 2009.

[16] Robert Saxon 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, 2007.

[17] Alexey Mkrtychev. Models for the logic of proofs. In Sergei Adian and Anil Nerode, editors, *Logical Foundations of Computer Science, 4th International Symposium, LFCS'97, Yaroslavl, Russia, July 6–12, 1997, Proceedings*, volume 1234 of *Lecture Notes in Computer Science*, pages 266–275. Springer, 1997.

[18] Eric Pacuit. A note on some explicit modal logics. In *Proceedings of the 5th Panhellenic Logic Symposium*, 2005.