Reduction of Modal Logic and Realization in Justification Logic

Hirohiko Kushida [1]

Computer Science Program, the Graduate Center, the City University of New York
365 Fifth Avenue, New York, NY, 10016, USA

Abstract

In this paper, we first offer basic results regarding modal logic: (1) a wide range of modal systems can be syntactically reduced to the modal logic K in terms of theoremhood and (2) we can restrict the forms of modal axioms without changing their deductive power in that range of modal logics. Then, based on these results, we offer a new, simple, uniform, and modular proof-theoretical proof of the realization of a wide range of modal logics with possible combinations of modal axioms $T, D, 4, 5$ (including S5) in Justification Logic. We do not use a generalization of sequent calculus, such as hypersequent and nested sequent calculi. We simply utilize the standard cut-free sequent calculus for K and then show, in the realized proof in Justification Logic (corresponding to K), how to recover the realizations of the modal axioms by rewriting terms in the proof.

Keywords: Modal Logic, Justification Logic, Proof Theory, Realization Theorem.

1 Introduction

One of the most common interpretations of modal logic is the epistemic logical interpretation: reading a modal formula $\Box A$ as "A is known." However, the machinery of epistemic logic does not refer to how the knowledge A is attained. Justification Logic offers a tool to refer to a reason or justification for a proposition; a modal formula is of the form $s : A$ with a term s, which is read as "s is a reason or justification for A." Moreover, Justification Logic is equipped with operators on terms: $+$, $\cdot$, ! and ?. The first two are binary and express the concatenation and an application of modus ponens, respectively; the latter two are unary and express positive and negative introspections, respectively. Then, for example, the logical omniscience problem could be avoided, in a sense; it could be viewed as a problem of term complexity. As we deduce a more complicated formula, we have a more complicated term with the formula at the same time. Cf. [6]. We refer to [3], [4], and [25] for a general introduction to the family of systems called Justification Logic.

[1] proof(underscore)hkushida@yahoo.co.jp

One of the fundamental results concerning Justification Logic is the realization theorem, which acts as a bridge to the modal logics. There have been many studies on the realization theorem for major modal logics. The realization theorem for the modal logic S4 was provided in Artemov [1], [2] with the Logic of Proofs, LP, which is the first system of Justification Logic. It makes the following claim: for some realization, that is, some assignment of terms to modality $\Box$, a formula is provable in S4 if and only if the realization of the formula is provable in LP. This result intended to give an arithmetical meaning to S4; a realized modal formula $s : A$ reads "s is a proof of A."

The original proof of the realization theorem in [1], [2] was a proof-theoretical one, using a standard cut-free sequent calculus of S4. Fitting [12] proposed a possible-world semantics for LP and proved the realization theorem using this semantics. The semantics has been studied well and extended for various systems of Justification Logic. It is called Fitting semantics today. Another semantical proof was offered for realization for LP in Fitting [15]. Substructural variants of LP were introduced, and the realization theorems were proved for some modal substructural logics by a proof-theoretic method in Kurokawa and Kushida [19].

Systems with the negative introspection operator were proposed by several authors pursuing epistemological interpretation of LP. Those systems correspond to the modal logic S5. Such a system was first introduced in Artemov et al. [5] and Kazakov [18], and the realization theorem for S5 was proved by a proof-theoretic method.

The negative introspection operator "?" that has been the subject of recent studies is characterized by the formula $\neg s : A \to ?s : \neg s : A$. It was proposed independently by Pacuit [27] and Rubtsova [28], [29]. The realization theorem was proved for S5 via Fitting semantics in [28], [29].

Fitting [14] offered an elegant proof-theoretical proof of the realization for S5 with the operator "?". Kurokawa and Kushida [20] offered an S5 variant of Linear Logic and proved the realization theorem for it with the corresponding substructural justification logic using a proof-theoretical method.

Nested sequent calculus is an apparatus used to execute an inference rule inside formulas. Although it is not clear if it is a natural expression of logical reasoning, it has been a useful tool to handle some logical systems that are not well-behaved proof-theoretically, such as S5. Motohashi [26] showed that the Intuitionistic Logic can be faithfully embedded in the classical predicate logic via a composition of Gödel's embedding and the standard translation (converting modality to quantifier). This result of [26] is one of the precursors of the method of nested sequent calculus, although it would be difficult to specify the first to have invented any similar kind of apparatus. In [21], the method was applied to a wide range of major modal logics between K and S5 (including the two) in a uniform way; it was shown that those modal logics can be faithfully embedded in the classical predicate logic by Motohashi's method. Later, we applied the method to the realization problem in light of Justification Logic in [22]; it was shown that the modal logic GL can be realized in a variant of LP with free variables using Motohashi's method.

While the realization of subsystems of S4 was proved in Brezhnev [8] proof-theoretically, a proof for modal logics including S5 was offered in a uniform way in Brünnler, Goetschi, and Kuznets [10]; Goetschi and Kuznets [17]; and Borg and Kuznets [7]. They utilized nested sequent systems to prove the realization for a wide range of modal logics between K and S5 (including the two). In particular, the proof in [7] was modular as well as uniform.

In this paper, we offer a new, simple, uniform, and modular proof of the realization of major modal logics extended by additional axioms: what we call $D, T, 4, 5$. These systems are modal logic correspondents to Justification Logic with the above-mentioned operators: $\cdot, +, !, ?$. [2] Our proof is a proof-theoretical one, but we do not use a generalization of sequent calculus, such as nested or hypersequent calculus; rather, we will simply use the standard cut-free sequent calculus for the modal logic K. We will present a reduction theorem of all of those extended modal logics over K. This result is concerned with the research problem treated in Fitting [11] and will be of independent interest apart from Justification Logic and the realization problem. Moreover, we will point out that the form of axioms $D, T, 4, 5$ can be restricted to a kind of normal form without changing their deductive power. This is a basic fact of the nature of modal logic, which seems not to have been published so far. We present the second reduction theorem using this normal form.

Then, we will make a realization for K to a basic system of Justification Logic called J. Then, to obtain realization for the other logics, we will show how to convert some realized formulas to the form of the axioms of Justification Logic by rewriting terms in the proof of a realized formula in J. It will be seen that a circular argument can be avoided in the rewriting algorithm, thanks to the second reduction theorem.

This paper is organized as follows. In §2, we define the modal logics treated in this study. Then, we offer two reduction theorems. It is also pointed out that the well-known modal axioms can be restricted to a sort of normal form. In §3, we define the systems of Justification Logic corresponding to those modal logics and prove the internalization theorem for a basic system of Justification Logic. In §4, we present our proof-theoretic proof of the realization theorem for all the systems defined in a uniform and modular way.

2 Modal Logics and Reduction Theorem

Let us begin with a review of axiomatic systems of the modal logic K and its normal extensions which we are going to handle in this paper. We adopt the propositional connectives: $\rightarrow, \neg$. The other ones are defined in terms of the two, which will be also used below. The unary modal operator $\Box$ is added. The other

[2] We do not handle the modal axiom called "B". We restrict our attention to terms with these operators in Justification Logic, while a new operator is needed to realize systems including "B", as was shown in [17], [7]. However, it is possible to apply our method to prove the realization for those systems including "B". We will touch on this point later in a footnote.

operator $\Diamond$ can be defined in terms of $\Box$, which is not considered in this paper. We use the symbols $\bot$ for the propositional constant and $P, Q, \ldots, P_1, P_2, \ldots$ for propositional variables. The formulas are constructed from atomic formulas in the usual way.

The modal logic K is an axiomatic system for the propositional logic augmented with the axiom $\Box(A \to B) \to (\Box A \to \Box B)$ and the inference rule $A/\Box A$ (Necessitation). We consider axioms called $D, T, 4$ and 5.

D	$\neg\Box\bot$
T	$\Box A \to A$
4	$\Box A \to \Box\Box A$
5	$\neg\Box A \to \Box\neg\Box A$

Then we obtain from K the system $\mathsf{KS}_1 \cdots \mathsf{S}_n$ extended with $S_1 \cdots S_n$ from the schemas $D, T, 4, 5$. As usual, we follow the custom to call the systems KD, KT, KT4, KT5 as D, T, S4, S5, respectively. (KT45 is equivalent to KT5.) By the notation $\mathsf{KS}_1 \cdots \mathsf{S}_n$, we can cover ten systems: D, T, K4, K5, K45, KD4, KD5, KD45, S4, S5. Let L denote any system from these systems.

Now, we show that L can be syntactically reduced to the modal logic K with respect to theoremhood. For L, a finite set of modal formulas α and a natural number n, we define the special formula $X(\alpha, n, \mathsf{L})$ as follows.

L	$X(\alpha, n, \mathsf{L})$
D	$\bigwedge_{0\le i\le n} \Box^i\neg\Box\bot$
T	$\bigwedge_{\Box B\in\alpha}\bigwedge_{0\le i\le n} \Box^i(\Box B \to B)$
K4	$\bigwedge_{\Box B\in\alpha}\bigwedge_{0\le i\le n} \Box^i(\Box B \to \Box\Box B)$
K5	$\bigwedge_{\Box B\in\alpha}\bigwedge_{0\le i\le n} \Box^i(\neg\Box B \to \Box\neg\Box B)$
K45	$X(\alpha, n, \mathsf{K4}) \wedge X(\alpha, n, \mathsf{K5})$
KD4	$X(\alpha, n, \mathsf{D}) \wedge X(\alpha, n, \mathsf{K4})$
KD5	$X(\alpha, n, \mathsf{D}) \wedge X(\alpha, n, \mathsf{K5})$
KD45	$X(\alpha, n, \mathsf{KD4}) \wedge X(\alpha, n, \mathsf{K5})$
S4	$X(\alpha, n, \mathsf{T}) \wedge X(\alpha, n, \mathsf{K4})$
S5	$X(\alpha, n, \mathsf{T}) \wedge X(\alpha, n, \mathsf{K5})$

Here "$\Box^n$" denotes "$\overbrace{\Box\cdots\Box}^{n-many}$".

Lemma 2.1 *Let α, β be any finite set of modal formulas and n, m be any natural numbers. Then we have the following.*

(1) $\vdash_{\mathsf{K}} X(\alpha\cup\beta, max(n,m), \mathsf{L}) \to X(\alpha, n, \mathsf{L}) \wedge X(\beta, m, \mathsf{L})$;

(2) $\vdash_{\mathsf{K}} X(\alpha, n+1, \mathsf{L}) \to \Box X(\alpha, n, \mathsf{L})$.

Proof. For (1). Suppose $n \ge m$. For any formula C, we have the following derivation by propositional calculus.

$$\begin{aligned} \bigwedge_{\Box B\in\alpha\cup\beta}\bigwedge_{0\le i\le n}\Box^i C \quad &\to \quad \bigwedge_{\Box B\in\alpha}\bigwedge_{0\le i\le n}\Box^i C \wedge \bigwedge_{\Box B\in\beta}\bigwedge_{0\le i\le n}\Box^i C \\ &\to \quad \bigwedge_{\Box B\in\alpha}\bigwedge_{0\le i\le n}\Box^i C \wedge \bigwedge_{\Box B\in\beta}\bigwedge_{0\le i\le m}\Box^i C \end{aligned}$$

Thus, we have proven the cases when L is D, T, $\mathsf{K4}$ or $\mathsf{K5}$. By using these results, we can prove the other cases; we handle the case L is $\mathsf{KD5}$. (Other cases are similar.) We have the following derivation by propositional calculus.

$$\begin{array}{rcc} X(\alpha \cup \beta, n, \mathsf{KD5}) & = & X(\alpha \cup \beta, n, \mathsf{D}) \wedge X(\alpha \cup \beta, n, \mathsf{K5}) \\ & \rightarrow & X(\alpha, n, \mathsf{D}) \wedge X(\beta, m, \mathsf{D}) \wedge X(\alpha, n, \mathsf{K5}) \wedge X(\beta, m, \mathsf{K5}) \\ & \rightarrow & X(\alpha, n, \mathsf{KD5}) \wedge X(\beta, m, \mathsf{KD5}) \end{array}$$

Thus, (1) holds for this case.

For (2). When L is D, T, $\mathsf{K4}$ or $\mathsf{K5}$. For any formula C, we have the following derivation in K.

$$\begin{array}{rcl} \bigwedge_{\Box B \in \alpha} \bigwedge_{0 \leq i \leq n+1} \Box^i C & \rightarrow & \bigwedge_{\Box B \in \alpha} \bigwedge_{1 \leq i \leq n+1} \Box^i C \\ & \rightarrow & \Box \bigwedge_{\Box B \in \alpha} \bigwedge_{0 \leq i \leq n} \Box^i C \end{array}$$

Thus, (2) holds for these cases.

The other cases can be established by using these results; again, we take the case $\mathsf{L} = \mathsf{KD5}$ only, as the remaining cases are similarly proved. We have the following derivation in K.

$$\begin{array}{rcc} X(\alpha, n+1, \mathsf{KD5}) & = & X(\alpha, n+1, \mathsf{D}) \wedge X(\alpha, n+1, \mathsf{K5}) \\ & \rightarrow & \Box X(\alpha, n, \mathsf{D}) \wedge \Box X(\alpha, n, \mathsf{K5}) \\ & \rightarrow & \Box[X(\alpha, n, \mathsf{D}) \wedge X(\alpha, n, \mathsf{K5})] \\ & = & \Box X(\alpha, n, \mathsf{KD5}) \end{array}$$

Thus, this case has been proven for (2). □

We call '$\Box A$' in the above definition of $D, T, 4, 5$ *the core* of them. E.g., $\Box(\Box P \wedge \neg P)$ is the core of an axiom T: $\Box(\Box P \wedge \neg P) \rightarrow (\Box P \wedge \neg P)$. For a given proof in L, we define $\mathcal{AS}$ (*axiom specification*) to be the set $\{\Box A : \Box A$ is the core of an axiom $D, T, 4$ or 5 used in the proof$\}$.

Lemma 2.2 *For any formula A of modal logic, if $\vdash_{\mathsf{L}} A$ with some $\mathcal{AS}$, then $\vdash_{\mathsf{K}} X(\mathcal{AS}, n, \mathsf{L}) \rightarrow A$, for some n.*

Proof. We proceed by induction on the length of a proof of A in L with $\mathcal{AS}$. When the proof is an axiom of K, $X(\mathcal{AS}, n, \mathsf{L}) = \emptyset$. When the proof is an axiom of D, T, 4 or 5, $\vdash_{\mathsf{K}} X(\mathcal{AS}, 0, \mathsf{L}) \rightarrow A$.

• For modus ponens, suppose that A is derived from $B \rightarrow A$ and B. By the induction hypothesis, for some $\mathcal{AS}_1, \mathcal{AS}_2, n$ and m, we have $\vdash_{\mathsf{K}} X(\mathcal{AS}_1, n, \mathsf{L}) \rightarrow (B \rightarrow A)$ and $\vdash_{\mathsf{K}} X(\mathcal{AS}_2, m, \mathsf{L}) \rightarrow B$. Then, we obtain $\vdash_{\mathsf{K}} X(\mathcal{AS}_1, n, \mathsf{L}) \wedge X(\mathcal{AS}_2, m, \mathsf{L}) \rightarrow A$. By (1) of Lemma 2.1, $\vdash_{\mathsf{K}} X(\mathcal{AS}_1 \cup \mathcal{AS}_2, max(n, m), \mathsf{L}) \rightarrow A$.

• For necessitation, suppose that $A = \Box B$ is derived from B. By the induction hypothesis, for some $\mathcal{AS}$ and n, we have $\vdash_{\mathsf{K}} X(\mathcal{AS}, n, \mathsf{L}) \rightarrow B$. By necessitation and normality of '$\Box$', we obtain $\vdash_{\mathsf{K}} \Box X(\mathcal{AS}, n, \mathsf{L}) \rightarrow \Box B$. By (2) of Lemma 2.1, $\vdash_{\mathsf{K}} X(\mathcal{AS}, n+1, \mathsf{L}) \rightarrow \Box B$. □

Theorem 2.3 *(the first Reduction Theorem) For any formula A of modal logic, the following two are equivalent.*

(1) $\vdash_{\mathsf{L}} A$ *with* $\mathcal{AS}$*;*
(2) $\vdash_{\mathsf{K}} X(\mathcal{AS}, n, \mathsf{L}) \to A$*, for some* n*.* [3]

Proof. It is easily seen that, for any α and any n, $X(\alpha, n, \mathsf{L})$ is provable in L. Then, (2) obviously implies (1). The converse direction immediately follows from Lemma 2.2. □

We take an example to sketch a reduction of proof in $\mathsf{KD5}$ to that in K in Appendix I.

2.1 Restriction of Modal Axioms

Here, we show that modal logics under consideration have the same deductive power if we restrict the form of the axioms in a certain way. We define a normal form of formulas of modal logic as follows.

Definition 2.4 *The normal form of formulas is defined as follows.*

1. $P_1 \wedge \cdots \wedge P_n \to Q_1 \vee \cdots \vee Q_p$ *is in normal form.*
2. *When* $B_1, \ldots, B_m, C_1, \ldots, C_q$ *are in normal form, so is the following:* $P_1 \wedge \cdots \wedge P_n \wedge \Box B_1 \wedge \cdots \wedge \Box B_m \to Q_1 \vee \cdots \vee Q_p \vee \Box C_1 \vee \cdots \vee \Box C_q$
3. *If* B *is equivalent (in propositional logic) to a formula in normal form,* B *is also in normal form.*

Theorem 2.5 *(Normal Form Theorem) For any formula* A *of modal logic,* A *is equivalent in* K *to a conjunction of formulas in normal form.*

Proof. We define the *degree* of A, $d(A)$, as follows. $d(P) = 0; d(A \to B) = d(A) + d(B); d(\neg A) = d(A); d(\Box A) = d(A) + 1$. We proceed by induction on $d(A)$. At first, by propositional logic, A can be transformed into a conjunction of the forms:

$$(\natural) \quad P_1 \wedge \cdots \wedge P_n \wedge \Box B_1 \wedge \cdots \wedge \Box B_m \to Q_1 \vee \cdots \vee Q_p \vee \Box C_1 \vee \cdots \vee \Box C_q.$$

Here, by this propositional transformation, the formulas (each B_i and each C_j) inside the outmost occurrences of □ are untouched.

Now, in the base case, A is a conjunction of the form $P_1 \wedge \cdots \wedge P_n \to Q_1 \vee \cdots \vee Q_p$ and is in normal form. In the induction step, let D denote any B_i or any C_j. By the induction hypothesis, D can be equivalently in K transformed into the form $E_1 \wedge \cdots \wedge E_r$ with each E_i in normal form. Hence, $\vdash_{\mathsf{K}} \Box D \leftrightarrow \Box(E_1 \wedge \cdots \wedge E_r) \leftrightarrow \Box E_1 \wedge \cdots \wedge \Box E_r$. So, we may assume that each B_i in ($\natural$) is already in normal form. As to C_j in ($\natural$), assume that $C_1 = E_1 \wedge \cdots \wedge E_r$ where each E_i is in normal form. Then, ($\natural$) is equivalent to the following.

$$\bigwedge_{1 \le i \le r} [P_1 \wedge \cdots \wedge P_n \wedge \Box B_1 \wedge \cdots \wedge \Box B_m \to Q_1 \vee \cdots \vee Q_p \vee \Box E_i \vee \Box C_2 \vee \cdots \vee \Box C_q]$$

After all, A is equivalent in K to a conjunction of the forms of ($\natural$) where each B_i and each C_j are in normal form. □

[3] We could restrict the set of modal formulas $\mathcal{AS}$ so that the elements come from subformulas of A rather than axioms of a proof in L of A. This direction of research is found in [11]. Here, we cannot make such a restriction because our axiomatic systems do not enjoy the subformula property. Anyway, our concern here lies in the realization of modal logics and constructing $\mathcal{AS}$ this way is enough for our purpose.

We show that the restriction of the core of modal axioms to normal form does not change the deductive power of systems.

Theorem 2.6 *If $\vdash_{\mathsf{L}} A$, then $\vdash_{\mathsf{L}} A$ with $\mathcal{AS}$ consisting of formulas in normal form.*

Proof. It suffices to show that a general form of axiom of T, 4 and 5, respectively, is derivable in K from a restricted form of T, 4 and 5 with the core in normal form, respectively. By the Normal Form Theorem, a formula B is equivalent to $E_1 \wedge \cdots \wedge E_r$ with each E_i in normal form. Note that E_i is in normal form if and only if $\Box E_i$ is in normal form.

On T axiom: we have $\vdash_{\mathsf{K}} \Box B \to B = \Box(E_1 \wedge \cdots \wedge E_r) \to (E_1 \wedge \cdots \wedge E_r). \leftrightarrow (\Box E_1 \wedge \cdots \wedge \Box E_r) \to (E_1 \wedge \cdots \wedge E_r)$. Also, we have $\vdash_{\mathsf{K}} [(\Box E_1 \to E_1) \wedge \cdots \wedge (\Box E_r \to E_r)] \to .(\Box E_1 \wedge \cdots \wedge \Box E_r) \to (E_1 \wedge \cdots \wedge E_r)$. Therefore, $\vdash_{\mathsf{K}} [(\Box E_1 \to E_1) \wedge \cdots \wedge (\Box E_r \to E_r)] \to .\Box B \to B$.

On 4 axiom, it is similar to the case of T axiom.

On 5 axiom, we have $\vdash_{\mathsf{K}} \neg\Box B \to \Box\neg\Box B = \neg\Box(E_1 \wedge \cdots \wedge E_r) \to \Box\neg\Box(E_1 \wedge \cdots \wedge E_r). \leftrightarrow (\neg\Box E_1 \vee \cdots \vee \neg\Box E_r) \to \Box(\neg\Box E_1 \vee \cdots \vee \neg\Box E_r)$. On the other hand, $\vdash_{\mathsf{K}} [(\neg\Box E_1 \to \Box\neg\Box E_1) \wedge \cdots \wedge (\neg\Box E_r \to \Box\neg\Box E_r)] \to .(\neg\Box E_1 \vee \cdots \vee \neg\Box E_r) \to (\Box\neg\Box E_1 \vee \cdots \vee \Box\neg\Box E_r)$. As $\Box F \vee \Box G$ implies $\Box(F \vee G)$ in K for any F and G, we obtain $\vdash_{\mathsf{K}} [(\neg\Box E_1 \to \Box\neg\Box E_1) \wedge \cdots \wedge (\neg\Box E_r \to \Box\neg\Box E_r)] \to .\neg\Box B \to \Box\neg\Box B.\Box$

Now, we can sharpen the Reduction Theorem.

Theorem 2.7 *(the second Reduction Theorem) For any formula A of modal logic, the following two are equivalent.*

(1) $\vdash_{\mathsf{L}} A$;

(2) $\vdash_{\mathsf{K}} X(\alpha, n, \mathsf{L}) \to A$, for some α and n such that α consists of formulas in normal form.

Proof. Derived by Theorems 2.3 and 2.6. □

Each of Theorems 2.3, 2.5, 2.6, 2.7 is a simple but general observation and would belong to basics of modal logic, although it seems not commonly known. Theorem 2.7 will be useful to give a uniform proof of realization theorem in the following sections and could be thought of to reveal a hidden nature of modal logics together with the realization. [4]

3 Justification Logics and Internalization

Next, we review the corresponding systems of Justification Logic. The formulas of Justification Logic are defined in the same way as modal logic except that

---

[4] As we remarked in the Introduction, we do not handle the axiom "B" of the form $\neg A \to \Box\neg\Box A$. Anyway, the whole argument in this section holds for "B" and the systems with it, and the realization for systems with "B" can be proved by our method in the following sections. However, unfortunately, the modal logics GL and GLS do not satisfy Theorems 2.6 or 2.7, while they do Theorem 2.3 where we have the definitions: $X(\alpha, n, \mathsf{GL}) = \bigwedge_{\Box B \in \alpha} \bigwedge_{0 \le i \le n} \Box^i(\Box(\Box B \to B) \to \Box B)$ and $X(\alpha, n, \mathsf{GLS}) = X(\alpha, n, \mathsf{GL}) \wedge \bigwedge_{\Box B \in \alpha}(\Box B \to B)$. See [23] for a recent development of the study of GLS.

$\Box A$ is replaced with $s : A$, where s is a justification term, or simply, term and defined inductively as follows.

1. Constants $c, d, e, \ldots, c_1, c_2, \ldots$ are justification terms.
2. Variables $x, y, z, \ldots, x_1, x_2, \ldots$ are justification terms.
3. If s and t are justification terms, then so are $s \cdot t, s + t, !s$, and $?s$.

For $\boldsymbol{t} = (t_1, \ldots, t_n)$, by $\cdot(\boldsymbol{t})$ we mean any concatenation of all terms of $(t_1, \ldots, t_n)$ via the operator $\cdot$ in arbitrary order. The term $+(\boldsymbol{t})$ is similarly defined with $+$ in place of $\cdot$. The basic system J is defined by the following axioms and inference rules.

Axioms:
A1. Axioms of classical propositional logic
A2. $s : (A \to B) \to .t : A \to (s \cdot t) : B$
A3. $s : A \to (s + t) : A; \quad t : A \to (s + t) : A$

Rules of Inference:
R1. Modus Ponens: $A, A \to B / B$
R2. Iterated Axiom Necessitation: $A / c_1 : c_2 : \cdots : c_n : A$,
where each c_i $(1 \leq i \leq n)$ is a constant and A is an axiom.

The *constant specification*, CS, in a proof is defined to be the set of formulas introduced by R2 in the proof. We introduce the axioms named $D^j, T^j, 4^j, 5^j$ as follows.

D^j	$\neg s : \bot$
T^j	$s : A \to A$
4^j	$s : A \to !s : s : A$
5^j	$\neg s : A \to ?s : \neg s : A$

For modal logic $\mathsf{L} = \mathsf{KS}_1 \cdots \mathsf{S}_n$, the system JL is provided by J augmented with the axioms: $S_1^j, \ldots, S_n^j$.

Let us prove the internalization theorem for J, which is a fundamental property of Justification Logics. Below, for any term s and formula A, by $at(s)$ and $at(A)$ we mean a set of atomic terms (that is, constants and variables) appearing in s and A, respectively.

Theorem 3.1 *(Internalization for J) For any formula A of J,* $\vdash_J A$ *implies* $\vdash_J \cdot(\boldsymbol{c}) : A$, *for some term of the form* $\cdot(\boldsymbol{c})$ *such that* $at(\cdot(\boldsymbol{c})) \cap at(A) = \emptyset$.

Proof. We proceed by induction on the length of a proof of A in J. When the proof is an axiom itself, we can take any fresh constant c so that $c : A$ is provable in J by R2. In the induction step, for the case of R1, by the induction hypothesis, we have terms $\cdot(\boldsymbol{c})$ and $\cdot(\boldsymbol{d})$ such that the following hold.

$\vdash_J \cdot(\boldsymbol{c}) : A \qquad \vdash_J \cdot(\boldsymbol{d}) : (A \to B)$
$at(\cdot(\boldsymbol{c})) \cap at(A) = \emptyset \qquad at(\cdot(\boldsymbol{d})) \cap at(A \to B) = \emptyset$

If $at(\cdot(\boldsymbol{c})) \cap at(B) \neq \emptyset$, we can substitute fresh constants for some of $\boldsymbol{c}$ to make it empty. (This is possible because any constants of $\boldsymbol{c}$ are introduced in R2 and we can choose any constants in applying R2.) By using A2 and R1, we have $\vdash_J (\cdot(\boldsymbol{c}) \cdot \cdot(\boldsymbol{d})) : B$ and $at(\cdot(\boldsymbol{c}) \cdot \cdot(\boldsymbol{d})) \cap at(B) = \emptyset$.

For the case of R2, when we have $c_n : c_{n-1} : \cdots : c_1 : A$ from an axiom A, we can also have $c_{n+1} : c_n : c_{n-1} : \cdots : c_1 : A$ from A by R2. Here, c_{n+1} is a fresh constant and the desired term. □

We note that Theorem 3.1 is a refinement of the standard form of the Internalization Theorem, which just claims that provability of A implies provability of $s : A$ for some term s.

The following corollary follows straightforwardly; we put the proof to Appendix II due to the lack of space.

Corollary 3.2 *For any formulas $B_1, B_2, \ldots, B_n, A$ and any terms $t_1, t_2, \ldots, t_n$ of* J*,*
$\vdash_J B_1 \wedge B_2 \wedge \cdots \wedge B_n . \to A$ *implies* $\vdash_J t_1 : B_1 \wedge t_2 : B_2 \wedge \cdots \wedge t_n : B_n . \to [\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_n] : A$*, for some justification term* $\cdot(\boldsymbol{c})$ *such that* $at(\cdot(\boldsymbol{c})) \cap at(A) = \emptyset$*.* [5]

4 Realization of modal logics

A realization of a formula of modal logic is a replacement of each occurrence of □ in the formula with a justification term. Such a realization is denoted by r (possibly with integer subscripts) and the result of realization r for a formula A is denoted by A^r. Our aim is to prove the following realization theorem for L.

Theorem 4.1 *For any formula A of modal logic,*
$\vdash_L A$ *iff, for some* r, $\vdash_{JL} A^r$.

We are going to prove Theorem 4.1 by reducing it to the following Theorem 4.2 (the realization of K).

Theorem 4.2 *For any formula A of modal logic,*
$\vdash_K A$ *iff, for some* r, $\vdash_J A^r$.

Theorem 4.2 was first proved in Brezhnev [8] by utilizing sequent calculus method initiated by Artemov [2]. We modify the method slightly and naturally; the operator + will be used when two positive occurrences of □ merge in a proof in K.

We make use of the standard sequent calculus for K. A sequent is of the form $\Gamma \Longrightarrow \Delta$. [6] The sequent calculus for K, which we also call K, is defined to be the extension of the sequent calculus for classical propositional logic LK with the following rule. (See, for example, [30] for the full description of LK.)

---

[5] Here, we follow the notation of "association to the left" in restoring brackets of the form $s_1 \cdot s_2 \cdot \cdots \cdot s_m$. That is, $s_1 \cdot s_2 \cdot \cdots \cdot s_m$ is read as $(\cdots((s_1 \cdot s_2) \cdot s_3) \cdot \cdots \cdot s_m)$. On the other hand, $\cdot(\boldsymbol{c})$ is read according to our previous definition of this notation; it can be any term consisting of constants $\boldsymbol{c}$ and the operator $\cdot$.

[6] As usual, by greek capital letters, we mean finite sequences of formulas.

$$\frac{\Gamma \Longrightarrow A}{\Box\Gamma \Longrightarrow \Box A}\ \Box$$

We assume the well-known facts: (i) this sequent calculus is equivalent to the axiomatic system K with respect to theoremhood and (ii) it enjoys the cut-elimination theorem.

For a sequent $S = \Gamma \Longrightarrow \Delta$, its *formula image*, $fi(S)$, is defined to be $\bigwedge\Gamma \to \bigvee\Delta$.

Proof of Theorem 4.2. The 'if' part is proved by using what is called the forgetful projection, say f: for any formula B of modal logic and any realization r, $(B^r)^f = B$. It is easily shown that $(A^r)^f = A$ is provable in K by induction on the length of a proof of A^r in J.

Now we handle the other part. Let us recall the 'normality' of realization introduced in [2]. A normal realization of a formula is one that assigns a variable to each negative occurrence of $\Box$. A realization of a sequent $S = \Gamma \Longrightarrow \Delta$ is defined by: $S^r = (fi(S))^r$. S^r can be also expressed by $\Gamma^r \Longrightarrow \Delta^r$. r for S is normal if S^r is normal.

Let P be a cut-free proof of S in K. In P, we restrict the initial sequent $A \Longrightarrow A$ to the case when A is an atomic formula. For an application of inference rule, an occurrence of $\Box$ in a upper sequent has the (obviously) related occurrence of $\Box$ in the lower sequent. Thus, all occurrences of $\Box$ form a 'forest' in P, where occurrences of $\Box$ are nodes and in-between inference rules are edges. Each occurrence of $\Box$ in the end-sequent is the 'root' of a 'tree'. All of the occurrences of $\Box$ belonging to a specific 'tree' have the same polarity. We call a tree which has positive occurrences of $\Box$ a *positive tree* and one which has negative occurrences of $\Box$ a *negative tree* in P.

We present the Realization Algorithm which assigns a term to each occurrence of $\Box$ in P so that each realized sequent is provable in J.

Realization Algorithm

(Step 1) Assign distinct variables to each negative tree in P, and replace all the nodes $\Box$ in a tree with the assigned variable.

(Step 2) Fix a positive tree in P. We proceed from top to bottom.

2.1. Assign a distinct variable for each leaf of the tree which is introduced by the rule '$\Box$'. Also, assign a uniform variable to all leaves of the tree which are introduced otherwise.

2.2. Keep on assigning the same term in each branch until another branch meets with it or the root is reached.

2.2.1. When two branches of the tree merge by 'c' (contraction) or logical rules, connect the two obtained terms by the operator $+$ and assign the new term to the next node. We take an example of the case when 'c' is involved.

$$\frac{B(\Box C), B(\Box C), \Gamma \Longrightarrow \Delta}{B(\Box C), \Gamma \Longrightarrow \Delta}\ c$$

Here, $\Box C$ occurs negatively in B and positively in the whole sequent. Suppose that one indicated occurrence of $\Box$ of $\Box C$ is replaced with $+(\boldsymbol{x})$ and the other is replaced with $+(\boldsymbol{y})$. Then, replace the related occurrence of $\Box$ in the lower sequent with $[+(\boldsymbol{x})] + [+(\boldsymbol{y})]$.

(Step 3) Update r by replacing variables x used in (Step 2) for the leaves of positive trees introduced by $\Box$ rule as follows.

$$\frac{B_1, \ldots, B_n \Longrightarrow C}{\Box B_1, \ldots, \Box B_n \Longrightarrow \Box C}\ \Box$$

Suppose that $(\Box B_1, \ldots, \Box B_n \Longrightarrow \Box C)^r$ has become $y_1 : B_1^r \wedge \cdots \wedge y_n : B_n^r \to x : C^r$ in (Step 1, 2). By Corollary 3.2, there is some $\cdot(\boldsymbol{d})$ such that if $B_1^r \wedge \cdots \wedge B_n^r . \to C^r$ is provable in J then so is $y_1 : B_1^r \wedge \cdots \wedge y_n : B_n^r \to (\cdot(\boldsymbol{d}) \cdot y_1 \cdot \cdots \cdot y_n) : C^r$. Update r so that $\cdot(\boldsymbol{d}) \cdot y_1 \cdot \cdots \cdot y_n$ is substituted for x.

(The end of the Realization Algorithm)

It is easily seen that this algorithm halts eventually. Also, it surely works correctly. We put the argument for the correctness in Appendix III.

In this way, we can obtain a normal realization of a formula provable in K such that the resulting formula is provable in J. This completes the proof of Theorem 4.2. $\Box$

We note the following point on the normal realization we have constructed from a cut-free proof in K in the proof of Theorem 4.2.

Note. We can take fresh constants for $\cdot(\boldsymbol{d})$ in (Step 3) for each application of rule $\Box$, because those constants are introduced from the rule R2 and we can choose any constant in applying R2. Thus, each leaf in a positive tree is realized to a term which does not share variables or constants with other leaves, and they can merge with the operator + in 'c' or logical inferences, while in the original algorithm in [2], all the nodes in a positive tree have the same term.

Proof of Theorem 4.1. For the 'if' part, it is similarly proved to Theorem 4.2. For the 'only if' part. Suppose that A is provable in L. In light of the second Reduction Theorem (Theorem 2.7), there is a cut-free proof P in K of $X_1, \ldots, X_p \Longrightarrow A$. Here, $X(\alpha, n, \mathsf{L}) = X_1 \wedge \cdots \wedge X_p$ for some n and some set α composed of formulas in normal forms; each X_i is $X(\alpha, n, \mathsf{D})$, $X(\alpha, n, \mathsf{T})$, $X(\alpha, n, \mathsf{K4})$ or $X(\alpha, n, \mathsf{K5})$.

Fix any X_a. We impose the following condition.

(♮♮) There is no application of $c : l$ (contraction on the left hand side) in P on any subformula of X_a.

We can transform P so that (♮♮) is satisfied; any such application of $c : l$ can be permuted with the following inference so that X_a may be duplicated in the end-sequent. We show this. Proceed from top to bottom. We distinguish cases by the inference below such an application of $c : l$, among which we pick up two cases: $\to$: r and $\Box$. When it is $\to$: r, we can move the application of

$c : l$ to the right by permuting them, as follows.

$$\dfrac{\dfrac{A, A, \Gamma \Rightarrow \Delta, B}{A, \Gamma \Rightarrow \Delta, B}\; c:l}{\Gamma \Rightarrow \Delta, A \to B}\; \to: r \quad \rhd \quad \dfrac{\dfrac{\dfrac{\dfrac{A, A, \Gamma \Rightarrow \Delta, B}{A, \Gamma \Rightarrow \Delta, A \to B}\; \to: r}{A, \Gamma \Rightarrow \Delta, A \to B, B}\; w}{\Gamma \Rightarrow \Delta, A \to B, A \to B}\; \to: r}{\Gamma \Rightarrow \Delta, A \to B}\; c:r$$

When it is the rule $\Box$, we can exchange it with the application of $c : l$, as follows.

$$\dfrac{\dfrac{A, A, \Gamma \Rightarrow B}{A, \Gamma \Rightarrow B}\; c:l}{\Box A, \Box\Gamma \Rightarrow \Box B}\; \Box \quad \rhd \quad \dfrac{\dfrac{A, A, \Gamma \Rightarrow B}{\Box A, \Box A, \Box\Gamma \Rightarrow \Box B}\; \Box}{\Box A, \Box\Gamma \Rightarrow \Box B}\; c:l$$

After all, we may suppose that $(\natural\natural)$ holds. Now we apply the Realization Algorithm to the proof P to obtain a proof, say P^*, in J of $X_1^r, \ldots, X_p^r \Longrightarrow A^r$ with some normal realization r. Fix any X_a. X_a has one of the forms:

$\Box^i(\Box B \to B)$;
$\Box^i(\Box B \to \Box\Box B)$;
$\Box^i(\neg\Box B \to \Box\neg\Box B)$.

Here, B is in normal form and can be $\bot$. Each form has two occurrences of a formula B such that the corresponding occurrences of $\Box$ have the opposite polarities inside B. Thus, the normal realization of them can be different: B^{r1} and B^{r2}. The realization of X_a is one of the forms:

$x_1 : \cdots x_i : (u : B^{r2} \to B^{r1})$;
$x_1 : \cdots x_i : (u : B^{r2} \to y_1 : y_2 : B^{r1})$;
$x_1 : \cdots x_i : (\neg y_1 : B^{r1} \to y_2 : \neg u : B^{r2})$.

Our first task is to reconcile B^{r1} and B^{r2} by rewriting terms in P^* and so updating the realization. If B contains no $\Box$, there is nothing to do here. Also, propositional variables are unimportant for the task. Thus, we may suppose that B is of the form:

$$\Box C_1 \wedge \cdots \wedge \Box C_n \to \Box D_1 \vee \cdots \vee \Box D_m$$

Here, each C_i and D_j are in normal form. Suppose that B^{r1} and B^{r2} are of the following forms.

$$B^{r1} = s_1 : C_1^r \wedge \cdots \wedge s_n : C_n^r \to z_1 : D_1^r \vee \cdots \vee z_m : D_m^r$$
$$B^{r2} = w_1 : C_1^r \wedge \cdots \wedge w_n : C_n^r \to t_1 : D_1^r \vee \cdots \vee t_m : D_m^r$$

By induction on $deg(B)$, we show that the realization can be so updated that (i) B^{r1} and B^{r2} are identical, and (ii) the realization of other parts of $X(\alpha, n, \mathsf{L}) \to A$ than X_a can change in such a way that only positive occurrences of a variable are replaced with a term.

As a result, the realization will be no longer normal. By the induction hypothesis, we assume that the realizations of each C_i and D_j in B^{r1} and B^{r2} are identical. We apply the following algorithm.

Rewriting Algorithm

(Step 1) For all $1 \leq i \leq n$, replace w_i in P^* with s_i. For all $1 \leq j \leq m$, let t_j^+ be a term obtained from t_j by this replacement.

(Step 2) For all $1 \leq j \leq m$, replace z_j in P^* with t_j^+.

(The end of Rewriting Algorithm)

Clearly, this algorithm halts eventually, as occurrences to be replaced are finite in each step and the number of those occurrences is reduced after each replacement. Also, the algorithm works correctly; we put the detailed argument in Appendix IV. Here, we note that (Step 1) and (Step 2) essentially reconcile the antecedent of B^{r1} and B^{r2} and the succedent of B^{r1} and B^{r2}, respectively, and (Step 2) does not change that antecedent anymore (as no s_i contains any z_j), thanks to the second Reduction Theorem and the property (♮♮). This is why we could avoid a circular argument in reconciling B^{r1} and B^{r2}. [7]

Also, note that (Step 1, 2) both take the form: for negative occurrences of variables, replace all (negative and positive) occurrences of them with some term. So, even if some preceding application of this Rewriting Algorithm to another conjunct altered some variables which occur only positively in the conjunct X_a^r under consideration it does not lose the applicability of the Rewriting Algorithm to X_a^r.

We have updated the realization r, which is not normal now, so that $X(\alpha, n, \mathsf{L})^r \to A^r$ is provable in J where each conjunct X_a^r of $X(\alpha, n, \mathsf{L})^r$ is of the following form.

$x_1 : \cdots x_i : (u : B^r \to B^r)$;
$x_1 : \cdots x_i : (u : B^r \to y_1 : y_2 : B^r)$;
$x_1 : \cdots x_i : (\neg y_1 : B^r \to y_2 : \neg u : B^r)$.

Our remaining task is to make these forms provable in JL. First, for each conjunct X_a, there are outermost realized modalities, $x_1, \ldots, x_i$. Take fresh constants $c_1, \ldots, c_i$. For each $1 \leq a \leq i$, replace x_a in P^* with c_a. Then, we distinguish cases according to L. $X(\alpha, n, \mathsf{L}) - X(\alpha, n, \mathsf{L}_0)$ is a formula obtained from $X(\alpha, n, \mathsf{L})$ by removing $X(\alpha, n, \mathsf{L}_0)$. For systems L_0 and L_1, we write $\mathsf{L}_0 \subseteq \mathsf{L}_1$ to mean the latter extends the former.

(Case 1) When $\mathsf{D} \subseteq \mathsf{L}$, $\neg u : \bot$ is an axiom in JL. By R2, $c_1 : \cdots c_i : (\neg u : \bot)$ is provable in JL. Therefore, $\vdash_{\mathsf{JL}} X(\alpha, n, \mathsf{L})^r - X(\alpha, n, \mathsf{D})^r . \to A^r$.

(Case 2) When $\mathsf{T} \subseteq \mathsf{L}$, $u : B^r \to B^r$ is an axiom in JL, and, by R2, $\vdash_{\mathsf{JL}} c_1 : \cdots c_i : (u : B^r \to B^r)$. Therefore, $\vdash_{\mathsf{JL}} X(\alpha, n, \mathsf{L})^r - X(\alpha, n, \mathsf{T})^r . \to A^r$.

(Case 3) When $\mathsf{K4} \subseteq \mathsf{L}$, first replace y_1 and y_2 in P^* with u and $!u$, respectively. Then, $u : B^r \to !u : u : B^r$ is an axiom in JL and, by R2, $c_1 : \cdots c_i : (u : B^r \to !u : u : B^r)$ is provable in JL. Hence, $\vdash_{\mathsf{JL}} X(\alpha, n, \mathsf{L})^r - X(\alpha, n, \mathsf{K4})^r . \to A^r$.

(Case 4) When $\mathsf{K5} \subseteq \mathsf{L}$, first replace y_1 and y_2 in P^* with u and $?u$, respectively. Then, $\neg u : B^r \to ?u : \neg u : B^r$ is an axiom in JL. By applying R2, $\vdash_{\mathsf{JL}} c_1 :$

[7] The second Reduction Theorem and the property (♮♮) are actually based on the same idea: we can rule out positive occurrences of $\wedge$ in modal axioms without changing deductive power. (They are negative in the whole sequent.)

$\cdots c_i : (\neg u : B^r \to ?u : \neg u : B^r)$. Hence, $\vdash_{\mathsf{JL}} X(\alpha, n, \mathsf{L})^r - X(\alpha, n, \mathsf{K5})^r. \to A^r$.

The obtained figure is surely a proof in J, because all replacement we executed is so that variables are converted to terms. Each conjunct of $X(\alpha, n, \mathsf{L})^r$ is now of the following form.

$c_1 : \cdots c_i : (u : B^r \to B^r)$;
$c_1 : \cdots c_i : (u : B^r \to !u : u : B^r)$;
$c_1 : \cdots c_i : (\neg u : B^r \to ?u : \neg u : B^r)$.

In this way, we can eliminate every conjunct of $E(\alpha, n, \mathsf{L})^r$ in JL and we obtain the result of provability of A^r in JL. This finishes the proof of Theorem 4.1. □

The realization which we finally constructed is not normal. However, it is obtained from the normal realization we obtained through the Realization Algorithm by assigning terms to variables. Thus, positive occurrences of terms are still composed of negative occurrences of terms. In this sense, the final realization would keep a flavor of normality.

5 Conclusion Remark

In this paper, we offered the reduction theorems of modal logics to the system K, and we proved a basic fact that modal axioms can be restricted to a sort of normal form without changing their deductive power. Then, based on these results, we presented a uniform and modular proof of the realization of major modal logics in Justification Logics using a proof-theoretical method.

As further research problems, it would be intriguing to clarify a semantical meaning of the reduction theorems and normal form theorem (in terms of both possible-world and algebraic semantics.) Also it would be interesting to investgate the extension of the theorems to second-order modal logics. Moreover, it would be intriguing to ask how far our method can be generalized, as recently it turned out in Fitting [16] that there exist infinitely many modal logics that have counterparts in Justification Logic. [8]

Appendix

I. *Example of reduction of proof.*

Here we sketch an example of reduction (as in Theorem 2.3) of proof in KD5 to that in K. Let us consider the formula $\Box(\neg P \vee \neg\Box Q) \to \Box\Box\neg\Box(P \wedge Q)$ provable in KD5. We permit (i) putting hypotheses in a proof, where of course we cannot apply Necessitation to a formula depending on hypotheses and (ii) applying an inference rule introducing '$\to$' discharging some hypotheses, a conjunction of which occur as the antecedent of the introduced '$\to$'. This relaxation is justifiable in the standard axiomatic system for propositional logic and, therefore, our system K. Here is a sketch of its proof in KD5.

[8] The question concerning algebraic model was suggested to me by an anonymous referee.

1. $\Box(\neg P \vee \neg\Box Q)$ *Hypothesis*

⋮

n_1. $\neg\Box Q \to \Box\neg\Box Q$ *Axiom* 5

⋮

n_2. $\Box(\neg P \vee \Box\neg\Box Q)$

⋮

n_3. $\neg\Box\neg\Box Q \to \Box\neg\Box\neg\Box Q$ *Axiom* 5

⋮

n_4. $\Box(\Box\neg P \vee \Box\neg\Box Q)$

⋮

n_5. $\neg\Box\bot$ *Axiom D*

⋮

n_6. $\Box(\neg\Box P \vee \Box\neg\Box Q)$

⋮

n_7. $\neg\Box P \to \Box\neg\Box P$ *Axiom* 5

⋮

n_8. $\Box(\Box\neg\Box P \vee \Box\neg\Box Q)$

⋮

n_9. $\Box\Box\neg\Box(P \wedge Q)$

n_{10}. $\Box(\neg P \vee \neg\Box Q) \to \Box\Box\neg\Box(P \wedge Q)$ 1

Then, we can convert this proof to the following proof in K.

1. $[\Box(\neg P \vee \neg\Box Q)]$ *Hypothesis*

⋮

n_1. $\Box(\neg\Box Q \to \Box\neg\Box Q)$ *Hypothesis*

⋮

n_2. $\Box(\neg P \vee \Box\neg\Box Q)$

⋮

n_3. $\Box(\neg\Box\neg\Box Q \to \Box\neg\Box\neg\Box Q)$ *Hypothesis*

⋮

n_4. $\Box(\Box\neg P \vee \Box\neg\Box Q)$

⋮

n_5. $\Box\neg\Box\bot$ *Hypothesis*

⋮

n_6. $\Box(\neg\Box P \vee \Box\neg\Box Q)$

⋮

n_7. $\Box(\neg\Box P \to \Box\neg\Box P)$ *Hypothesis*

⋮

n_8. $\Box(\Box\neg\Box P \vee \Box\neg\Box Q)$

⋮

n_9. $\Box\Box\neg\Box(P \wedge Q)$

n_{10}. $\Box(\neg P \vee \neg\Box Q) \to \Box\Box\neg\Box(P \wedge Q)$ 1

n_{11}. $X(\alpha, 1, \mathsf{KD5})^- \to .\Box(\neg P \vee \neg\Box Q) \to \Box\Box\neg\Box(P \wedge Q)$ n_1, n_3, n_5, n_7

⋮

n_{12}. $X(\alpha, 1, \mathsf{KD5}) \to .\Box(\neg P \vee \neg\Box Q) \to \Box\Box\neg\Box(P \wedge Q)$

Here, $X(\alpha, 1, \mathsf{KD5})^-$ is a conjunction of the formulas n_1, n_3, n_5, n_7 and

$\alpha = \{\Box Q, \Box\neg\Box Q, \Box\bot, \Box P\}$. Note that $X(\alpha, 1, \mathsf{KD5}) = X(\alpha, 0, \mathsf{KD5}) \wedge X(\alpha, 1, \mathsf{KD5})^{-}$.

II. *Proof of Corollary 3.2.*

Suppose $\vdash_{\mathsf{J}} B_1 \wedge B_2 \wedge \cdots \wedge B_n. \rightarrow A$. Then, $\vdash_{\mathsf{J}} B_1 \rightarrow (B_2 \rightarrow \cdots (B_n \rightarrow A)\cdots)$. By Theorem 3.1, for some $\cdot(\boldsymbol{c})$, $\vdash_{\mathsf{J}} \cdot(\boldsymbol{c}) : [B_1 \rightarrow (B_2 \rightarrow \cdots (B_n \rightarrow A)\cdots)]$ such that $at(\cdot(\boldsymbol{c})) \cap at(A) = \emptyset$. We work in J and by induction on n. Suppose that we obtain:

$$t_1 : B_1 \rightarrow .t_2 : B_2 \rightarrow . \cdots t_i : B_i \rightarrow \\ (\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_i) : [B_{i+1} \rightarrow (\cdots (B_n \rightarrow A)\cdots)].$$

The following is an axiom from A2.

$$(\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_i) : [B_{i+1} \rightarrow (\cdots (B_n \rightarrow A)\cdots)] \rightarrow . \\ t_{i+1} : B_{i+1} \rightarrow (\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_i \cdot t_{i+1}) : [B_{i+2} \rightarrow (\cdots (B_n \rightarrow A)\cdots)]$$

Then, by propositional calculus with the last two formulas, we obtain:

$$t_1 : B_1 \rightarrow .t_2 : B_2 \rightarrow . \cdots t_i : B_i \rightarrow .t_{i+1} : B_{i+1} \rightarrow \\ (\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_i \cdot t_{i+1}) : [B_{i+2} \rightarrow (\cdots (B_n \rightarrow A)\cdots)].$$

Thus, we have:

$$t_1 : B_1 \rightarrow .t_2 : B_2 \rightarrow . \cdots t_n : B_n \rightarrow (\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_n) : A.$$

and, by propositional calculus,

$$t_1 : B_1 \wedge t_2 : B_2 \wedge \cdots \wedge t_n : B_n. \rightarrow (\cdot(\boldsymbol{c}) \cdot t_1 \cdot t_2 \cdot \cdots \cdot t_n) : A.$$

Here, the desired property on terms is preserved.

III. *Argument for the correctness of the Realization Algorithm.*

We verify the correctness of the algorithm: every realized sequent obtained in there is provable in J. We proceed from top to bottom in P. For an initial sequent S of the form $A \Longrightarrow A$ or $\bot, \Gamma \Rightarrow \Delta$, S^r is an axiom of J. It is easily checked that for every application of a rule, if the realizations of the upper sequents are provable in J then so is that of the lower sequent, except the case when two branches of a positive tree merge via 'c' or logical inferences. These cases are similarly treated. We handle the case of $\wedge : r$ here.

$$\frac{B(\Box C), \Gamma \Longrightarrow \Delta, D \quad B(\Box C), \Gamma \Longrightarrow \Delta, E}{B(\Box C), \Gamma \Longrightarrow \Delta, D \wedge E} \wedge : r$$

Here, $\Box C$ occurs negatively in B and positively in the whole sequent. Suppose that the upper sequent is realized as follows.

$$B^r(s : C^r), \Gamma^r \Longrightarrow \Delta^r, D^r \qquad B^r(t : C^r), \Gamma^r \Longrightarrow \Delta^r, E^r$$

It is easily seen that we can replace the related occurrences of s (the indicated term of $s : C^r$), corresponding to some branches of the positive tree in P, with $s + t$, keeping all the inferences in J; and we can do the same for the related occurrences of t (the indicated term of $t : C^r$), corresponding to other branches of the positive tree in P. Then we obtain a proof of the realized sequent

$$B^r((s+t):C^r),\Gamma^r \Longrightarrow \Delta^r, D^r \qquad B^r((s+t):C^r),\Gamma^r \Longrightarrow \Delta^r, E^r$$

Thus, we can know the realization of the lower sequent of $\wedge : r$ is provable by propositional inferences (corresponding to $\wedge : r$) in J.

IV. *Argument for correctness of the Rewriting Algorithm.*

We consider only the case of the conjunct $X_a = \Box^i(\Box B_{(2)} \to B_{(1)})$. The other cases can be treated similarly. Let $B_{(1)}$ and $B_{(2)}$ be occurrences of B which have become B^{r1} and B^{r2} by the realization, respectively. In the proof P in K, there can be some applications of $\to: l$ to introduce $\Box B_{(2)} \to B_{(1)}$.

$$\begin{array}{cc} P_1 & P_2 \\ \vdots & \vdots \end{array}$$

$$\frac{\Gamma \Longrightarrow \Delta, \Box B_{(2)} \quad B_{(1)}, \Gamma \Longrightarrow \Delta}{\Box B_{(2)} \to B_{(1)}, \Gamma \Longrightarrow \Delta} \to: l$$

$$\vdots$$

$$\Box^i(\Box B_{(2)} \to B_{(1)}), X^-(\alpha, n, \mathsf{L}) \Longrightarrow A$$

In the subproof P_1, there can be applications of $\to: r$ introducing $B_{(2)}$.

$$\vdots$$

$$\frac{\Box C_1 \wedge \cdots \wedge \Box C_n, \Sigma \Longrightarrow \Theta, \Box D_1 \vee \cdots \vee \Box D_m}{\Sigma \Longrightarrow \Theta, \Box C_1 \wedge \cdots \wedge \Box C_n \to \Box D_1 \vee \cdots \vee \Box D_m} \to: r$$

$$\vdots$$

$$\Gamma \Longrightarrow \Delta, \Box B_{(2)}$$

By the Realization Algorithm, the principal formula of such an application of $\to: r$ becomes of the form:

$$w_1 : C_1^r \wedge \cdots \wedge w_n : C_n^r \to t_1' : D_1^r \vee \cdots \vee t_m' : D_m^r$$

Here, each t_i' is a subterm of the corresponding t_i in B^{r2}; they become identical when more $+$ are added.

Fix any w_i $(1 \leq i \leq n)$. We show w_i does not appear in any C_j^r or D_k^r.

There can be several occurrences of $\Box C_i$ the $\Box$ of which belongs to the same negative tree and is realized to w_i. Since they must be contracted eventually in P, it cannot appear in any C_j or D_k.

Also, there can be occurrences of $\Box E$ which is the right principal formula of applications of $\Box : r$ having a left principal formula $\Box C_i$ and is realized to w_i. $\Box E$ may be some $\Box D_k$. Two formulas (C_j and $\Box E$) ($j = i$ or $j \neq i$) and (D_k and $\Box E$) are never contracted in cut-free P. This is because to contract such two, C_j of $\Box C_j$ or D_k of $\Box D_k$ must have $\Box E$ as a subformula and $\Box E$ should have one more $\Box$ outside itself. However, since the rule $\Box$ increases the number of $\Box$ by one for each auxiliary formula, $\Box C_j$ or $\Box D_k$ would have also one more $\Box$ outside. Thus, such two formulas are never contracted. [9]

Hence, firstly, the realization inside each C_i and D_k does not use any variable w_i ($1 \leq i \leq n$), and (Step 1) does not change the realization of any C_i or D_k. [10]

Next, the root of the negative tree which is associated with w_i appears inside X_a and is obviously the only negative occurrence of w_i in the end-sequent, while the roots of the positive trees associated with terms containing w_i can appear inside or outside $X_a = \Box^i(\Box B_{(2)} \to B_{(1)})$ in the end-sequent. So, secondly, for other part of $X(\alpha, n, \mathsf{L}) \to A$ than X_a, (Step 1) can replace only the positive occurrences of variables of $w_i (1 \leq i \leq n)$.

Thus, the execution of (Step 1) guarantees that the antecedents of B^{r1} and B^{r2} become identical and satisfies the desired property (ii).

Concerning (Step 2), we turn to look at P_2. In the subproof P_2, there can be applications of $\to: l$ introducing $B_{(1)}$.

$$\vdots$$

$$\dfrac{\Sigma \Longrightarrow \Theta, \Box C_1 \wedge \cdots \wedge \Box C_n \qquad \Box D_1 \vee \cdots \vee \Box D_m, \Sigma \Longrightarrow \Theta}{\Box C_1 \wedge \cdots \wedge \Box C_n \to \Box D_1 \vee \cdots \vee \Box D_m, \Sigma \Longrightarrow \Theta} \to: l$$

$$\ddots \;\vdots\; \therefore$$

$$B_{(1)}, \Gamma \Longrightarrow \Delta$$

By the Realization Algorithm, the principal formula of such an application of $\to: l$ becomes of the form:

$$s'_1 : C^r_1 \wedge \cdots \wedge s'_n : C^r_n \to z_1 : D^r_1 \vee \cdots \vee z_m : D^r_m$$

[9] This is formally proved by induction on the number of applications of rules between each $\Box$ rule which introduce some $\Box C_j$ and the end-sequent.

[10] In other words, we do not have a self-referential realization on any $\Box C_i$ and $\Box D_k$. Generally, this kind of self-reference phenomenon can be avoided in realization of the modal logic K and D, which was shown in Kuznets [24]. Here, we proved the possibility to avoid self-referentiality for a specific form of formulas in a cut-free proof in K.

Here, each s'_i is a subterm of the corresponding one in B^{r1}; they become identical when more $+$ are added.

Fix any z_i $(1 \leq i \leq m)$. There can be applications of $\Box$-rule which have $\Box D_i$ as a left principal formula. Let $\Box E$ be the right principal formula of any such application of $\Box$-rule. By a similar argument to P_1, $\Box E$ cannot merge with any C_j or D_k. So, the realization does not use any z_i there, and (Step 2) does not change any C_j^r or D_k^r.

Moreover, in the subproof above the left upper sequent of the application of $\rightarrow$: l, there is no such application of $\Box$-rule. Because: if there is, $\Box D_i$ appears in the lower sequent of it, it must be contracted below the $\rightarrow$: l with the occurrence of $\Box D_i$ in the right upper sequent of the $\rightarrow$: l, but it contradicts (♮♮). Therefore, $\Box E$ never merges with any $\Box C_i$. (So, what cannot merge with $\Box E$ is not only C_i but $\Box C_i$.) Hence, no term of s_j $(1 \leq j \leq n)$ contains any z_i, and (Step 2) does not change any s_j. This guarantees that (Step 2) does not change the outcome of (Step 1), and we obtain non circularity of the Rewriting Algorithm. [11]

Finally, by a similar argument to P_1, for other part of $X(\alpha, n, \mathsf{L}) \rightarrow A$ than X_a, (Step 2) can replace only the positive occurrences of variables of $z_i (1 \leq i \leq n)$.

Thus, the execution of (Step 2) guarantees that the succedents of B^{r1} and B^{r2} become identical, the antecedents remain untouched, and satisfies the desired property (ii). Note that after each step of the rewriting process, the obtained figure is surely a proof in J.

References

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

[2] Artemov S., Explicit provability and constructive semantics, The Bulletin of Symbolic Logic, 7(1), 2001, pp.1-36.

[3] Artemov, S. and Fitting, M.: Justification Logic, The Stanford Encyclopedia of Philosophy, 2012.

[4] Artemov, S. and Fitting, M.: Justification Logic: Reasoning with Reasons, Cambridge University Press, 2019.

[5] Artemov, S., E. Kazakov, and D. Shapiro. On logic of knowledge with justifications. Technical Report CFIS 99-12, Cornell University, 1999.

[6] Artemov, S., and R. Kuznets. "Logical omniscience as infeasibility." Annals of pure and applied logic 165, no. 1 (2014): 6-25.

[11] We can adopt another way to avoid a circular argument, instead of further transforming proof to satisfy (♮♮); we introduce a new operation on terms, say '$*$', and axioms: $s * t : A \rightarrow s : A$ and $s * t : A \rightarrow t : A$. ('$s * t : A$' has a natural meaning, 'both s and t are a justification for A'.) Then, in the Realization Algorithm, we can make the operation $*$ play the same role in negative trees as $+$ does in positive trees. More concretely, for a negative tree, put a distinct variable to each leaf, and use $*$ where two branches meet to concatenate the two terms. Then, no s_i does not contain any z_j because z_j never occurs in the subproof above the application of $\Box$-rule whose right principal formula is realized with s_i. Finally, we can eliminate all occurrences of the operation $*$ by assigning a fresh variable to each negative tree.

[7] Borg A., Kuznets R. (2015) Realization Theorems for Justification Logics: Full Modularity. In: De Nivelle H. (eds) Automated Reasoning with Analytic Tableaux and Related Methods. TABLEAUX 2015. Lecture Notes in Computer Science, vol 9323. Springer, Cham

[8] Brezhnev V., On explicit counterparts of modal logics, Technical Report CFIS 2000-05, Cornell University, 2000.

[9] Brezhnev, V. and R. Kuznets, Making knowledge explicit: How hard it is, Theoretical Computer Science, 357, pp. 23-34, 2006.

[10] Brünnler, K., R. Goetschi, R. Kuznets, A syntactic realization theorem for justification logics, in: L.D. Beklemishev, V. Goranko, V. Shehtman (Eds.), Advances in Modal Logic, vol. 8, College Publications, 2010, pp. 39–58.

[11] Fitting, M., Subformula results in some propositional modal logics. Studia Logica 37, 387-391 (1978) doi: 10.1007/BF02176170

[12] Fitting, M., The logic of proofs, semantically, Ann. Pure Appl. Logic 132 (1) (2005) 1-25.

[13] Fitting, M., Justification logics, logics of knowledge, and conservativity. Ann Math Artif Intell 53, 153-167 (2008)

[14] Fitting M. (2011) The Realization Theorem for S5: A Simple, Constructive Proof. In: van Benthem J., Gupta A., Pacuit E. (eds) Games, Norms and Reasons. Synthese Library (Studies in Epistemology, Logic, Methodology, and Philosophy of Science), vol 353. Springer, Dordrecht.

[15] Fitting M., Realization using the model existence theorem, Journal of Logic and Computation, Volume 26, Issue 1, February 2016, Pages 213–234.

[16] Fitting M., Modal logics, justification logics, and realization, Annals of Pure and Applied Logic, Volume 167, Issue 8, August 2016, Pages 615-648.

[17] Goetschi, R., Kuznets, R., Realization for justification logics via nested sequents: Modularity through embedding. Annals of Pure and Applied Logic 163(9), pp. 1271-1298, 2012.

[18] Kazakov, E. L., Logics of Proofs for S5, M.Phil. thesis, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, in Russian, 1999.

[19] Kurokawa, H. and H. Kushida, Substructural Logic of Proofs. In: Libkin L., Kohlenbach U., de Queiroz R. (eds) Logic, Language, Information, and Computation. WoLLIC 2013. Lecture Notes in Computer Science, vol 8071. Springer, Berlin, Heidelberg, 2013.

[20] Kurokawa, H. and H. Kushida, Resource Sharing Linear Logic, Journal of Logic and Computation, vol.30(1), pp 281-294, 2020.

[21] Kushida H., Applicability of Motohashi's Method to Modal Logics, Bulletin of the Section of Logic, Volume 34/3, 2005, pp. 121–134.

[22] Kushida, H., On the realization of the provability of logic, manuscript, 2007.

[23] Kushida, H., A Proof Theory for the Logic of Provability in True Arithmetic, to appear in: Studia Logica, 2019.

[24] Kuznets R., Self-Referential Justifications in Epistemic Logic, Journal of Philosophical Logic, 39, pp. 577-590, 2010.

[25] Kuznets, R. and T. Studer, Logics of Proofs and Justifications, College Publications, 2019

[26] Motohashi, N., A faithful interpretation of intuitionistic predicate logic in classical predicate logic, Commentarii Mathematici Universitatis Sancti Pauli 21 (1972), pp. 11–23.

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

[28] Rubtsova, N., Evidence reconstruction of epistemic modal logic S5. Lecture Notes in Computer Science, vol. 3967, pp. 313–321, 2006.

[29] Rubtsova, N., On Realization of graphic-modality by Evidence Terms, Journal of Logic and Computation, Volume 16, Issue 5, October 2006, Pages 671–684,

[30] Takeuti G., *Proof Theory,* Second edition, North-Holland, Amsterdam, 1987.