Completeness of Modal Proofs for First-Order Predicate Proofs

Tatsuya Abe

Department of Computer Science, The University of Tokyo
abet@is.s.u-tokyo.ac.jp

Characterizing modal logic in first-order predicate logic has been a hot research topic in mathematical logic. Van Benthem gave an elegant characterization such that the standard translation of modal formulas coincides with the class of first-order predicate formulas invariant for bisimulations. While he characterized modal formulas in first-order predicate logic, we characterize modal proofs in first-order predicate logic in this paper. To be concrete, we give a complete translation from a term calculus based on intuitionistic modal logic into Barendregt's λP. This characterization, identifying equality of proofs, is recently considered to be significant since a term calculus based on intuitionistic modal logic is expected to realize staged computation.

1 Introduction

Modal logic is derived from ordinary propositional logic to gain expressibility with modal operators. In Kripke semantics, while propositional logic is defined only with one world, the minimal modal logic K yields the class of frames, i.e., K has the notion of one-step reachability between any two worlds. Furthermore, we can define other formal systems e.g., T, K4, S4, and S5 by adding some axioms. The axioms give the notions of reflexivity, positive finite step reachability, finite step reachability, and connected components, respectively.

On the other hand, first-order predicate logic is enriched by quantifiers. A formula in first-order predicate logic is of the form of $\forall x.\,\tau$. Roughly speaking, a first-order predicate formula $\forall x.\,\tau$ is satisfied if there exists a structure satisfying τ for any element a of the structure substituted for x.

Many logicians have been interested in relations connecting the two enriching notions. In fact, it is well-known that modal logic is realized in first-order predicate logic. To be precise, van Benthem showed that a first-order predicate formula invariant for bisimulations was the result of the following translation of a modal formula and vice versa [26]:

$$\begin{aligned} \Phi_a(P) &= Pa \\ \Phi_a(\sigma \supset \sigma') &= \Phi_a(\sigma) \supset \Phi_a(\sigma') \\ \Phi_a(\Box\sigma) &= \forall b.\, Rab \supset \Phi_b(\sigma) \end{aligned}$$

where P is a propositional variable in modal logic and a unary predicate symbol in first-order predicate logic. Also, R is a binary predicate symbol. That is, we assume that the signature of first-order predicate logic is

$$\{\, P \mid P \text{ is a propositional variable in modal logic} \,\} \cup \{R\} \ .$$

While van Benthem clarified a relation between modal formulas and first-order predicate formulas via *the standard translation* Φ_a, we focus *proofs* in this paper. In general, proofs in logic correspond to programs in an appropriate functional language in the sense of Curry-Howard isomorphism [13]. Now we claim that it is significant to clarify equality between modal proofs. This is because some theoretical computer scientists expect a program based on modal logic to realize staged computation by regarding its modality as a kind of relation between stages [7].

Davies and Pfenning's work has inspired some computer scientists to construct term calculi equipped with various tastes. For example, Miyamoto and Igarashi gave a typed calculus for secure information flow [21]. However, any of such calculi was constructed syntactically and its semantics was given implicitly or operationally. It may be inevitable since Davies and Pfenning's calculus, the calculus adopted as a basis, was not shown to have an explicit semantics in their original paper. On the other hand, we give a term calculus based on modal logic with denotational semantics. Adopting our calculus as a basis for constructing a new calculus, one can formalize a term calculus on his semantics more denotationally. Our calculus is expected to be a new basis for constructing term calculi equipped with several tastes.

Furthermore, we characterize equality of modal proofs from another perspective. We embed our term calculus based on modal logic into Barendregt's λP, a term calculus based on first-order predicate logic, and investigate the behaviors of modal proofs in it. The embedding is defined as an extension of the standard translation Φ_a. The λP-calculus has been studied for more than fifteen years. The equality of λP-terms is the same as that of proofs in a traditional natural deduction system of first-order predicate logic via Curry-Howard isomorphism. A formal goal of this paper is to show soundness and completeness of the embedding.

This paper deals with intuitionistic logic in contrast to van Benthem's characterization for classical logic. Classical logic is more difficult than intuitionistic logic in the treatment of proofs, while classical logic is easier than

(unit)	$M = *$	if $\Gamma \vdash M : \top$
(left)	$\pi_1\langle M_1, M_2\rangle = M_1$	
(right)	$\pi_2\langle M_1, M_2\rangle = M_2$	
(product)	$\langle \pi_1 M, \pi_2 M\rangle = M$	
($\supset\beta$)	$(\lambda x.M)N = [N/x]M$	
($\supset\eta$)	$\lambda x.Mx = M$	if $x \notin \mathrm{fv}\, M$
($\Box\beta$)	$\mathrm{box}\ \boxed{\begin{matrix} x_1 \\ \vdots \\ x_{i-1} \\ x_i \\ x_{i+1} \\ \vdots \\ x_n \end{matrix}}\ \mathrm{be}\ \boxed{\begin{matrix} M_1 \\ \vdots \\ M_{i-1} \\ \mathrm{box}\,\overrightarrow{y}\ \mathrm{be}\ \overrightarrow{N}\ \mathrm{in}\ M_i \\ M_{i+1} \\ \vdots \\ M_n \end{matrix}}\ \mathrm{in}\ L = \mathrm{box}\ \boxed{\begin{matrix} x_1 \\ \vdots \\ x_{i-1} \\ \overrightarrow{y} \\ x_{i+1} \\ \vdots \\ x_n \end{matrix}}\ \mathrm{be}\ \boxed{\begin{matrix} M_1 \\ \vdots \\ M_{i-1} \\ \overrightarrow{N} \\ M_{i+1} \\ \vdots \\ M_n \end{matrix}}\ \mathrm{in}[M_i/x_i]L$	
($\Box\eta$)	$\mathrm{box}\ x\ \mathrm{be}\ M\ \mathrm{in}\ x = M$	

Table 1: Axioms for $\lambda\Box$

intuitionistic logic with respect to provability. Equality of proofs in intuitionistic logic has been characterized in various fields, e.g., λ-calculi, categorical semantics, game semantics, etc. On the other hand, studies on proofs in classical logic is now being developed [11, 22]. Since the studies are energetically being done, some elegant characterizations of classical proofs must be found in future. We believe that this work will give some contributions to various studies on classical modal proofs then. In fact, we envision that the calculus given in this paper can be extended to a calculus based on classical modal calculus according to personal communication with Kakutani [16].

Related Work. No work has dealt with classical modal proofs. An early work on intuitionistic modal proofs is found in Martini and Masini's paper [19]. Martini and Masini studied which natural deduction of modal logic is suitable for the construction of term calculi, and gave a term calculus based on intuitionistic S4.

Pfenning and Wong defined a term calculus by giving some equations in consideration of Curry-Howard isomorphism [23]. Furthermore, they obtained some syntactical results such as *subject reduction*.

Bierman and de Paiva, Bellin et al., and Alechina et al. gave definitions of intuitionistic S4, intuitionistic K, and constructive S4 in category theory, respectively [6, 5, 2]. In particular, Bierman and de Paiva gave a term calculus based on the class of cartesian closed categories with coproducts, monoidal comonads, and $\Box$-strong monads as seen later in this paper.

A term calculus based on classical modal proofs is being developed by Kakutani [16].

Outline. In Section 2 we give some formal notions, and formally establish the goal of this paper, based on motivation in Section 1. In Section 3 we explain a procedure for reaching the goal, and prove two important properties, strong normalization and confluence, on the way of the procedure. In Section 4 we give a proof of the goal. In Section 5 we refer to other modalities. In Section 6 we describe what have been accomplished and what have not been accomplished in this paper, and explain problems and solution candidates for the the problems.

2 Preliminary

First, we consider the following natural deduction system:

$$\tau ::= P \mid \top \mid \tau \wedge \tau \mid \tau \supset \tau \mid \Box\tau$$

$$\Gamma, \tau \rhd \tau$$

$$\Gamma \rhd \top \qquad \frac{\Gamma \rhd \sigma_1 \quad \Gamma \rhd \sigma_2}{\Gamma \rhd \sigma_1 \wedge \sigma_2}$$

$$\frac{\Gamma \rhd \sigma_1 \wedge \sigma_2}{\Gamma \rhd \sigma_1} \qquad \frac{\Gamma \rhd \sigma_1 \wedge \sigma_2}{\Gamma \rhd \sigma_2}$$

$$\frac{\Gamma, \sigma \rhd \sigma'}{\Gamma \rhd \sigma \supset \sigma'} \qquad \frac{\Gamma \rhd \sigma \supset \tau \quad \Gamma \rhd \sigma}{\Gamma \rhd \tau}$$

$$\frac{\Gamma \rhd \Box\rho_i\ (0 \le i \le n) \quad \rho_1, \ldots, \rho_n \rhd \sigma}{\Gamma \rhd \Box\sigma}$$

where P is a propositional variable and Γ denotes a set of formulas. We assume that the strength order of connectives is $\Box$, $\wedge$, and $\supset$. In the following, $\Gamma \vdash \tau$ means that $\Gamma \rhd \tau$ is derivable. As well we adopt this notation in other natural deduction systems.

Remark that $i = 0$ in the last rule is allowed. In the case of $i = 0$, the last rule is as follows,

$$\frac{\rhd\ \sigma}{\rhd\ \Box\sigma}\quad .$$

This is required by the fact that we can give a Hilbert-style formal system with the same provability as that of the natural deduction system. It is as follows,

$$\begin{array}{ll} \text{axioms:} & \top \\ & (\rho \supset \sigma \supset \tau) \supset (\rho \supset \sigma) \supset \rho \supset \tau \\ & \sigma \supset \tau \supset \sigma \\ & \sigma \wedge \tau \supset \sigma \\ & \sigma \wedge \tau \supset \tau \\ & \sigma \supset \tau \supset \sigma \wedge \tau \\ & \Box(\sigma \supset \tau) \supset \Box\sigma \supset \Box\tau \\ \text{inference rules:} & \sigma \supset \tau \text{ and } \sigma \text{ imply } \tau \\ & \sigma \text{ implies } \Box\sigma\ \ . \end{array}$$

The formal system is thus an intuitionistic fragment of the minimal logic K.

We define a term calculus $\lambda\Box$ based on modal logic by introducing proof terms to the natural deduction system:

$$\tau ::= P \mid \top \mid \tau \wedge \tau \mid \tau \supset \tau \mid \Box\tau$$

$$\Gamma, x\colon \tau \rhd x\colon \tau$$

$$\Gamma \rhd *\colon \top \qquad \frac{\Gamma \rhd M_1\colon \sigma_1 \quad \Gamma \rhd M_2\colon \sigma_2}{\Gamma \rhd \langle M_1, M_2\rangle\colon \sigma_1 \wedge \sigma_2}$$

$$\frac{\Gamma \rhd M\colon \sigma_1 \wedge \sigma_2}{\Gamma \rhd \pi_1 M\colon \sigma_1} \qquad \frac{\Gamma \rhd M\colon \sigma_1 \wedge \sigma_2}{\Gamma \rhd \pi_2 M\colon \sigma_2}$$

$$\frac{\Gamma, x\colon \sigma \rhd M\colon \sigma'}{\Gamma \rhd \lambda x^{\sigma}.M\colon \sigma \supset \sigma'} \qquad \frac{\Gamma \rhd M\colon \sigma \supset \tau \quad \Gamma \rhd N\colon \sigma}{\Gamma \rhd MN\colon \tau}$$

$$\frac{\Gamma \rhd N_i\colon \Box\rho_i\ (0 \le i \le n) \quad \overrightarrow{x\colon \rho} \rhd M\colon \sigma}{\Gamma \rhd \text{box}\ \overrightarrow{x^{\rho}}\ \text{be}\ \overrightarrow{N}\ \text{in}\ M\colon \Box\sigma}$$

where we often use the vector notation due to space limitation.

As remarked before, $i = 0$ is allowed in the last rule. At this time the rule is as follows,

$$\frac{\rhd\ M\colon \sigma}{\rhd\ \text{box be in}\ M\colon \Box\sigma}$$

although it may be seen a strange expression.

We use various notions of ordinary λ-calculi, e.g., binding, free variable, bound variable, α-conversion, and substitution. The notation is also similar to that in ordinary λ-calculi. In detail, see Barendregt's encyclopedic book [3]. In the following, α-convertible terms are identified syntactically (denoted by $\equiv$). However, it may be better to describe bindings in box-terms. Bindings in box-terms are the same as ones in let-terms in many programming languages, i.e., x^{ρ} binds free x^{ρ}s in M in "box x^{ρ} be N in M".

How should we define equality between proofs? It is surely a method giving some equations to identify two proofs which we want to identify. However, we commit equality of proofs to category theory, just as intuitionistic propositional logic is sound and complete to the class of cartesian closed categories. Kakutani and the author have constantly discussed term calculi based on modal logic committed to category theory. In the discussion Kakutani extracted axioms sound and complete to the class of cartesian closed categories with monoidal endofunctors. The axioms are as in Table 1 where we use embracing squares at some places in this paper, not as a syntax but for readability.

Furthermore, we consider the equations in Table 2. Intuitively, the former equation denotes *contraction* and the latter denotes *weakening.* It is said to be *the strongness condition* when these equations hold. The origin of the word depends on the fact that $\lambda\Box$ with the strongness condition is sound and complete to the class of cartesian closed categories with *strong* monoidal endofunctors [18, 16].

Next, let us recall Barendregt's λP [4] into which our modal calculus is embedded:

$$s ::= 1 \mid 2$$

$$\rhd\ 1\colon 2$$

$$\frac{\Gamma \rhd A\colon 1 \quad \Gamma, x\colon A \rhd B\colon s}{\Gamma \rhd \Pi x^{A}.B\colon s}$$

$$\frac{\Gamma \rhd A\colon s \quad x \notin \Gamma}{\Gamma, x\colon A \rhd x\colon A}$$

$$\frac{\Gamma \rhd A\colon B \quad \Gamma \rhd C\colon s \quad x \notin \Gamma}{\Gamma, x\colon C \rhd A\colon B}$$

$$\frac{\Gamma, x\colon A \rhd B\colon C \quad \Gamma \rhd \Pi x^{A}.C\colon s}{\Gamma \rhd \lambda x^{A}.B\colon \Pi x^{A}.C}$$

$$\frac{\Gamma \rhd D\colon \Pi x^{A}.B \quad \Gamma \rhd C\colon A}{\Gamma \rhd DC\colon [C/x]B}$$

$$\frac{\Gamma \rhd A\colon B \quad \Gamma \rhd B'\colon s \quad B = B'}{\Gamma \rhd A\colon B'}$$

where the relation $=$ is the smallest congruence relation containing $(\lambda x.B)C = [C/x]B$.

In the original notation, 1 and 2 are $*$ and $\Box$, respectively [4]. However, we do not adopt the original notation since $*$ and $\Box$ are confusing in this paper.

The λP-calculus is a term calculus based on intuitionistic first-order predicate logic just as LF is [12]. In this calculus, a type (e.g., Px) containing term variable (e.g., x) is a predicate (e.g., Px), and an abstraction (e.g., $\Pi x.Px$) is a universal formula (e.g., $\forall x.\,Px$). Types de-

$$\mathrm{box}\ \boxed{\begin{array}{c} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_{j-1} \\ x_j \\ x_{j+1} \\ \vdots \\ x_n \end{array}}\ \mathrm{be}\ \boxed{\begin{array}{c} N_1 \\ \vdots \\ N_i \\ \vdots \\ N_{j-1} \\ N_i \\ N_{j+1} \\ \vdots \\ N_n \end{array}}\ \mathrm{in}\ M = \mathrm{box}\ \boxed{\begin{array}{c} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_{j-1} \\ x_{j+1} \\ \vdots \\ x_n \end{array}}\ \mathrm{be}\ \boxed{\begin{array}{c} N_1 \\ \vdots \\ N_i \\ \vdots \\ N_{j-1} \\ N_{j+1} \\ \vdots \\ N_n \end{array}}\ \mathrm{in}[x_i/x_j]M$$

$$\mathrm{box}\ \boxed{\begin{array}{c} x_1 \\ \vdots \\ x_i \\ x_{i+1} \\ \vdots \\ x_n \end{array}}\ \mathrm{be}\ \boxed{\begin{array}{c} M_1 \\ \vdots \\ M_i \\ M_{i+1} \\ \vdots \\ M_n \end{array}}\ \mathrm{in}\ L = \mathrm{box}\ \boxed{\begin{array}{c} x_1 \\ \vdots \\ x_i \\ y \\ x_{i+1} \\ \vdots \\ x_n \end{array}}\ \mathrm{be}\ \boxed{\begin{array}{c} M_1 \\ \vdots \\ M_i \\ N \\ M_{i+1} \\ \vdots \\ M_n \end{array}}\ \mathrm{in}\ L\ .$$

Table 2: The strongness condition

pending on terms are called *dependent types*, which are directly supported in *Epigram* [9].

Now let us embed our modal calculi into λP. However, λP has only Π as connective by definition. Ordinarily, product types are indirectly defined on the way that it is extended to *higher-order*. Hence, it is not expected to embed $\lambda\Box$ and strong $\lambda\Box$ into λP without removing the unit type and product types. Also, λP does not have η-equations in origin. Therefore, let us consider the $\{\supset, \Box, \beta\}$-fragments of $\lambda\Box$ and strong $\lambda\Box$ in this paper, and call $\lambda\Box$ and strong $\lambda\Box$ de novo.

We extend the standard translation Φ_a to a function from not only *types* but also *terms* as in Table 3. In fact, we assume that propositional variables in $\lambda\Box$ and a binary predicate symbol R are signatures in λP. In this sense Φ_a is indeed a function to λP with constants.

The author expects the reader to accept that this translation is the most natural mapping to translate modal proofs in natural deduction style into λP-proofs. This Φ_a translates equations in strong $\lambda\Box$ into equations in λP as follows,

Theorem 2.1. *Assume that* $\Gamma \vdash M = M' : \tau$ *in strong* $\lambda\Box$. *Then* $\Phi_a(\Gamma) \vdash \Phi_a(M) = \Phi_a(M') : \Phi_a(\tau)$ *in* λP *where* $\Phi_a(x_1 : \sigma_1, \ldots x_n : \sigma_n)$ *denotes* $W : 1, a : W, x_1 : \Phi_a(\sigma_1), \ldots, x_n : \Phi_a(\sigma_n)$.

Now we are ready to establish our goal formally. Our goal in this paper is to show equality reflected in the image of Φ_a, i.e., completeness of Φ_a:

Theorem 2.2. *If* $\Phi_a(\Gamma) \vdash \Phi_a(M) = \Phi_a(M') : \Phi_a(\tau)$, *then* $\Gamma \vdash M = M' : \tau$ *in strong* $\lambda\Box$.

Completeness is often proved by the following procedure. Assume $\Phi_a(M) = \Phi_a(M')$. Next, construct an inverse function ${\Phi_a}^{-1}$ for the sound translation Φ_a. Finally, show that the inverse function preserves equality. Then,

$$M = {\Phi_a}^{-1}(\Phi_a(M)) = {\Phi_a}^{-1}(\Phi_a(M')) = M'$$

is derived. However, we had no idea to construct any inverse function to Φ_a. We therefore make a detour in the next section.

3 Strong Normalization and Confluence

In this section we show that any $\lambda\Box$-term can be identified with a $\lambda\Box$-term in normal form. For the purpose we give a reduction relation such that its reflexive, symmetric, and transitive closure coincides with the equality relation in $\lambda\Box$, and show strong normalization and confluence under the reduction relation.

First, we define a reduction relation by replacing $=$ of $(\supset\beta)$ and $(\Box\beta)$ with $\to$ in Table 1. In fact, the relation $\to$ is defined as the smallest compatible relation containing the above relation. Obviously the reflexive, symmetric, and transitive closure of $\to$ coincides with the equality relation in $\lambda\Box$.

Proposition 3.1. *If* $\Gamma \vdash M : \tau$ *and* $M \to M'$, *then* $\Gamma \vdash M' : \tau$.

$$\Phi_a(P) = Pa$$
$$\Phi_a(\sigma \supset \sigma') = \Pi x^{\Phi_a(\sigma)}.\Phi_a(\sigma')$$
$$\Phi_a(\Box\sigma) = \Pi b^W.\Pi u^{Rab}.\Phi_b(\sigma)$$

$$\Phi_a(x) = x$$
$$\Phi_a(\lambda x^\sigma.M) = \lambda x^{\Phi_a(\sigma)}.\Phi_a(M)$$
$$\Phi_a(MN) = \Phi_a(M)\Phi_a(N)$$
$$\Phi_a(\text{box}\,\overrightarrow{x^\rho}\,\text{be}\,\overrightarrow{N}\,\text{in}\,M) = \lambda b^W.\lambda u^{Rab}.(\lambda x_n.\cdots(\lambda x_1.\Phi_b(M))(\Phi_a(N_1)bu)\cdots)(\Phi_a(N_n)bu)$$

Table 3: A translation from $\lambda\Box$ into λP

We give the following terminologies, for convenience. M is said to be in normal form if $M \not\to M'$ for any M'. M is said to be have a normal form if $M \to^* M'$ and M' is in normal form. Of course, $\to^*$ is the reflexive and transitive closure of $\to$. M is strongly normalizable if there exists no infinite sequence $M_0, M_1, \ldots, M_n, \ldots$ such that $M \equiv M_0$ and $M_i \to M_{i+1}$ for any $i \in \omega$. A term calculus is strongly normalizable if all the typable terms are strongly normalizable.

Next, we will show strong normalization under the above relation $\to$. We reduce the strong normalization problem of $\lambda\Box$ to strong normalization of a term calculus. Let us recall a term calculus known to be strongly normalizable [24, 10, 8]:

$$\tau ::= P \mid \bot \mid \tau \supset \tau \mid \tau \vee \tau$$

$$\Gamma, x\colon \tau \rhd x\colon \tau$$

$$\frac{\Gamma, x\colon \sigma \rhd M\colon \sigma'}{\Gamma \rhd \lambda x.M\colon \sigma \supset \sigma'} \qquad \frac{\Gamma \rhd M\colon \sigma \supset \tau \quad \Gamma \rhd N\colon \sigma}{\Gamma \rhd MN\colon \tau}$$

$$\frac{\Gamma \rhd M\colon \sigma_1}{\Gamma \rhd \text{inl}\,M\colon \sigma_1 \vee \sigma_2} \qquad \frac{\Gamma \rhd M\colon \sigma_2}{\Gamma \rhd \text{inr}\,M\colon \sigma_1 \vee \sigma_2}$$

$$\frac{\Gamma \rhd N\colon \sigma_1 \vee \sigma_2 \quad \Gamma, x_i\colon \sigma_i \rhd M_i\colon \tau\ (i = 1, 2)}{\Gamma \rhd \text{case}\,N\,\text{of}\,x_1\,\text{in}\,M_1 \mid x_2\,\text{in}\,M_2\colon \tau}\ .$$

Here, $\bot$ does not express a contradiction but is merely a special symbol. Indeed, this calculus does not have the so-called *absurdity* rule, $\bot \vdash \tau$. The reduction relation is as in Table 4. We often use horizontal bars instead of vertical bars as separating symbols at some places in this paper, for readability. Let us call this calculus $\lambda\vee$ in this paper. For readers unfamiliar with strong normalization proofs, we note that easy proofs have recently studied for calculi containing *permutative conversions* [15, 8].

We give a translation from $\lambda\Box$ into $\lambda\vee$ as in Table 5.

Lemma 3.2. *If $\Gamma \vdash M\colon \tau$, then $[\![\Gamma]\!] \vdash [\![M]\!]\colon [\![\tau]\!]$.*

Lemma 3.3. *If $M \to M'$, then $[\![M]\!] \to^+ [\![M']\!]$ where $\to^+$ is the transitive closure of $\to$.*

Proof. See Appendix. ■

In fact, we have already reduced the strong normalization problem of $\lambda\Box$ to that of $\lambda\vee$ as follows,

Theorem 3.4. *$\lambda\Box$ is strongly normalizable.*

Proof. Assume that $\Gamma \vdash M_0\colon \tau$ and there exists a sequence $M_0, M_1, \ldots, M_n, \ldots$ such that $M_i \to M_{i+1}$ for any $i \in \omega$. By Lemma 3.2, $[\![\Gamma]\!] \vdash [\![M_0]\!]\colon [\![\tau]\!]$. In addition, $[\![M_i]\!] \to [\![M_{i+1}]\!]$ for any $i \in \omega$ by Lemma 3.3. These contradict the fact that $\lambda\vee$ is strongly normalizable. ■

Furthermore, we define the following terminologies. M and N are called confluent if there exists L such that $M \to^* L$ and $N \to^* L$. A term calculus is called confluent if any pair of typable equal terms is confluent.

Lemma 3.5. *All the critical pairs*[1] *are confluent.*

Proof. See Appendix. ■

Lemma 3.5 of a strongly normalizable calculus is called Knuth-Bendix's confluent condition. Knuth-Bendix's confluent condition implies confluence of $\lambda\Box$:

Theorem 3.6. *$\lambda\Box$ is confluent.*

Proof. By Theorem 3.4 and Lemma 3.5 [25]. ■

Corollary 3.7. *Any $\lambda\Box$-term has a unique normal form.*

Proof. By Theorems 3.4 and 3.6. ■

4 Completeness

Let us go back to the proof for completeness. The set of terms in normal form is formally defined by

$$F ::= x \mid FG$$
$$G ::= F \mid \lambda x^\sigma.G \mid \text{box}\,\overrightarrow{x^\rho}\,\text{be}\,\overrightarrow{F}\,\text{in}\,G\ .$$

[1]The terminology in term rewriting system is abused. In detail, see Terese's book [25].

$$(\lambda x.M)N \to [N/x]M$$
$$\text{case inl } N \text{ of } x_1 \text{ in } M_1 \mid x_2 \text{ in } M_2 \to [N/x_1]M_1$$
$$\text{case inr } N \text{ of } x_1 \text{ in } M_1 \mid x_2 \text{ in } M_2 \to [N/x_2]M_2$$
$$\text{case case } N \text{ of } \frac{y_1 \text{ in } M_1}{y_2 \text{ in } M_2} \text{ of } \frac{x_1 \text{ in } L_1}{x_2 \text{ in } L_2} \to \text{case } N \text{ of } \frac{y_1 \text{ in case } M_1 \text{ of } x_1 \text{ in } L_1 \mid x_2 \text{ in } L_2}{y_2 \text{ in case } M_2 \text{ of } x_1 \text{ in } L_1 \mid x_2 \text{ in } L_2}$$

Table 4: The reduction rules for $\lambda\vee$

Any $\lambda\Box$-term in normal form is not ambiguous in the above grammar. Therefore, a function Ψ_a from the set of terms in normal form can be inductively defined by

$$\Psi_a(x) = x$$
$$\Psi_a(\lambda x^\sigma.G) = \lambda x^{\Phi_a(\sigma)}.\Psi_a(G)$$
$$\Psi_a(FG) = \Psi_a(F)\Psi_a(G)$$
$$\Psi_a(\text{box } \overrightarrow{x^\rho} \text{ be } \overrightarrow{F} \text{ in } G) = \lambda b^W.\lambda u^{Rab}.\overrightarrow{[\Psi_a(F)bu/x]}\Psi_b(G) \ .$$

In general, $\Psi_a(G)$ does not coincide with $\Phi_a(G)$, e.g., $\Psi_a(\text{box } x^\rho \text{ be } y \text{ in } x^\rho) \not\equiv \Phi_a(\text{box } x^\rho \text{ be } y \text{ in } x^\rho)$. However, $\Psi_a(G)$ is always equal to $\Phi_a(G)$, i.e., $\Psi_a(G) = \Phi_a(G)$ holds. Furthermore, Ψ_a has the following pleasant property instead of being restricted to the set of normal forms.

Proposition 4.1. *Any λP-term in the image of Ψ_a is in normal form.*

Proof. Ψ_a translates applications and λ-abstractions of $\lambda\Box$ into applications and λ-abstractions of λP, respectively. Hence, we should take only $\overrightarrow{[\Psi_a(F)bu/x^\rho]}\Psi_b(G)$ into account. In fact, $\Psi_a(F)$ is not a λ-abstraction. Also, substituting applications for variables raises no redex. ■

We are ready to prove completeness in a partial sense.

Lemma 4.2. *If $\Phi_a(\Gamma) \vdash \Psi_a(G) = \Psi_a(G') : \Phi_a(\tau)$, then $\Gamma \vdash G = G' : \tau$ in strong $\lambda\Box$.*

Proof. Since λP is known to be strongly normalizable and confluent, $\Psi_a(G) = \Psi_a(G')$ means $\Psi_a(G) \equiv \Psi_a(G')$ by Proposition 4.1. By induction on G, we show that the set $\Psi_a{}^{-1}[\Psi_a(G)]$ is contained by the set of strong $\lambda\Box$-terms equal to G. Since W does not belong to the image of Φ_a, any term in the form $\lambda x^{\Phi_a(\sigma)}.\Psi_a(G)$ does not coincide with $\lambda b'^W.\lambda u'^{Ra'b'}.\overrightarrow{[\Psi_{a'}(F')b'u'/x']}\Psi_{b'}(G')$. It is therefore sufficient to consider only the case of $\overrightarrow{[\Psi_a(F)bu/x]}\Psi_b(G) \equiv \overrightarrow{[\Psi_a(F')bu/x']}\Psi_b(G')$ where the length of $\overrightarrow{x}$ may not be the same as the one of $\overrightarrow{x'}$.

Any G in the image of Ψ_b has no occurrence b except as an index for a variable. Also, b does not occur freely in $\Psi_a(F)$. We can therefore identify $\overrightarrow{\Psi_a(F)}$ whenever $\overrightarrow{[\Psi_a(F)bu/x]}\Psi_b(G)$ is given. The difference in substituting variables for $\overrightarrow{\Psi_a(F)}$ is collapsed by the strongness condition. ■

Our goal in this paper is accomplished as follows,

Proof of Theorem 2.2. Let G and G' be the normal forms of M and M' in $\lambda\Box$, respectively. By Theorem 2.1, $\Phi_a(M) = \Phi_a(G)$ holds. Also, $\Phi_a(G) = \Psi_a(G)$ holds as described. Similarly, consider the case of M'. Then, $\Psi_a(G) = \Psi_a(G')$ hold. This induces $G = G'$ in strong $\lambda\Box$ by Lemma 4.2. We finally obtain $M = M'$ in strong $\lambda\Box$. ■

5 On Other Modalities

As seen in Kakutani's paper [16], we can define a term calculus corresponding to intuitionistic T by adding a family of constants $\{\, \varepsilon^\tau : \Box\tau \supset \tau \,\}$ satisfying T in Table 6. In accordance with this, we add a family of constants $\{\, e_a : Raa \,\}$ into λP and extend Φ_a such that

$$\Phi_a(\varepsilon^\tau) = \lambda z^{\Pi b^W.\Pi u^{Rab}.\Phi_a(\tau)}.zae_a \ .$$

This Φ_a is sound, i.e., if $\Gamma \vdash M = M' : \tau$ in T, then $\Phi_a(\Gamma) \vdash \Phi_a(M) = \Phi_a(M') : \Phi_a(\tau)$ in λP.

Also, we can define a term calculus corresponding to intuitionistic K4 by adding a family of constants $\{\, \delta^\sigma : \Box\sigma \supset \Box\Box\sigma \,\}$ satisfying 4 in Table 6. In this case we can show the similar result by adding a family of constants $\{\, d_{abc} : \Pi u^{Rab}.\Pi v^{Rbc}.Rac \,\}$ and translate δ^σ into

$$\lambda z^{\Pi b^W.\Pi u^{Rab}.\Phi_a(\sigma)}.\lambda b^W.\lambda u^{Rab}.\lambda c^W.\lambda v^{Rbc}.zc(d_{abc}uv) \ .$$

However, we must take care to consider intuitionistic S4. The modality of intuitionistic S4 is considered to be a comonad on the analogy of the modality "!" of intuitionistic linear logic. It is therefore insufficient only to add T and 4. In fact, we add com_1 and com_2 in Table 6 and consider

$$d_{a_1a_3a_4}(d_{a_1a_2a_3}uv)w = d_{a_1a_2a_4}u(d_{a_2a_3a_4}vw)$$
$$d_{aab}e_au = d_{abb}ue_b = u$$

plus η-equations in λP.

Thus we can characterize some *normal* modal calculi by adding appropriate constants and their equations to λP.

$$
\begin{aligned}
[\![P]\!] &= P \\
[\![\sigma \supset \sigma']\!] &= [\![\sigma]\!] \supset [\![\sigma']\!] \\
[\![\Box\sigma]\!] &= [\![\sigma]\!] \vee \bot \\
\\
[\![x]\!] &= x \\
[\![\lambda x^{\sigma}.M]\!] &= \lambda x.[\![M]\!] \\
[\![MN]\!] &= [\![M]\!][\![N]\!]
\end{aligned}
$$

$$
[\![\mathrm{box}\ \overrightarrow{x^{\rho}}\ \mathrm{be}\ \overrightarrow{N}\ \mathrm{in}\ M]\!] = \mathrm{case}[\![N_n]\!]\ \mathrm{of}\ \frac{x_n\ \mathrm{in} \cdots \mathrm{case}[\![N_1]\!]\ \mathrm{of}\ \dfrac{x_1\ \mathrm{in}\ \mathrm{inl}[\![M]\!]}{w_1\ \mathrm{in}\ \mathrm{inr}\ w_1} \\ \vdots}{w_n\ \mathrm{in}\ \mathrm{inr}\ w_n}
$$

Table 5: A translation from $\lambda\Box$ into $\lambda\vee$

6 Conclusion

In this paper we clarified a relation between modal logic and first-order predicate logic at proof-level. Formally, we gave a complete translation from strong $\lambda\Box$ into λP as an extension of the standard translation from modal logic to first-order predicate logic. On the way of proving the completeness, we showed strong normalization and confluence of $\lambda\Box$. This is also a contribution.

We indeed proved completeness for only the $\{\supset, \Box, \beta\}$-fragment of intuitionistic modal calculus. In general, for any calculus complete to a class of cartesian closed categories it is very difficult to give an appropriate reduction relation whose reflexive, symmetric, and transitive closure is equality of the calculus. This is because reduction relations are often required to have the strong normalization and confluence properties for solving *the decision problem* of equality between terms. Also in this paper we showed strong normalization and confluence of $\lambda\Box$ for identifying any term with a term in normal form. However, calculi with the unit type $\top$ tend to fail either strong normalization or confluence [17].

For the purpose of repairing the defect, Mints switched some η-equations from η-reduction to η-expansion in the term calculus sound and complete to the class of cartesian closed categories [20]. Although it was not obvious that the term calculus was strongly normalizable and confluent, Jay and Akama proved it independently [14, 1]. We conjecture that via a similar method the full intuitionistic modal calculus can be completely embedded into intuitionistic first-order predicate calculus.

Acknowledgments. I am grateful to Yoshihiko Kakutani. He and I have constantly discussed various research topics in mathematical logic. This work is strongly due to the discussion. I also thank Masami Hagiya, Masahito Hasegawa, Ryu Hasegawa, Daisuke Kimura, and Koji Nakazawa for providing useful advice.

References

[1] Y. Akama. On Mints' reduction for ccc-calculus. In *Proceedings of the 1st International Conference on Typed Lambda Calculi and Applications*, volume 664 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 1993.

[2] N. Alechina, M. Mendler, V. de Paiva, and E. Ritter. Categorical and Kripke semantics for constructive S4 modal logic. In *Proceedings of the 15th International Workshop on Computer Science Logic*, volume 2142 of *Lecture Notes in Computer Science*, pages 292–307. Springer-Verlag, 2001.

[3] H. P. Barendregt. *The Lambda Calculus: Its Syntax and Semantics*. North-Holland, revised edition, 1984.

[4] H. P. Barendregt. *Lambda Calculi with Types*, volume 2 of *Handbook of Logic in Computer Science*, pages 117–309. Oxford University Press, 1992.

[5] G. Bellin, V. de Paiva, and E. Ritter. Extended Curry-Howard correspondence for a basic constructive modal logic. In *Proceedings of Methods for Modalities Conference*, 2001.

[6] G. M. Bierman and V. de Paiva. On an intuitionistic modal logic. *Studia Logica*, 65(3):383–416, 2000.

[7] R. Davies and F. Pfenning. A modal analysis of staged computation. *Journal of the ACM*, 48(3):555–604, 2001.

[8] P. de Groote. On the strong normalisation of intuitionistic natural deduction with permutation-conversions. *Information and Computation*, 178(2):441–464, 2002.

[9] Epigram Project. http://www.e-pig.org/.

[10] J.-Y. Girard, P. Taylor, and Y. Lafont. *Proofs and Types*. Cambridge University Press, 1989.

[11] T. G. Griffin. A formulae-as-types notion of control. In *Proceedings of the 17th Annual ACM Symposium on*

$$(T)\qquad \varepsilon^{\tau}\,\mathrm{box}\,\overrightarrow{x^{\sigma}}\,\mathrm{be}\,\overrightarrow{N}\,\mathrm{in}\,M = (\lambda x_n.\cdots(\lambda x_1.M)(\varepsilon^{\sigma_1}N_1)\cdots)(\varepsilon^{\sigma_n}N_n)$$

$$(4)\qquad \delta^{\sigma}\,\mathrm{box}\,\overrightarrow{x^{\rho}}\,\mathrm{be}\,\overrightarrow{N}\,\mathrm{in}\,M = \mathrm{box}\,\overrightarrow{y^{\Box\rho}}\,\mathrm{be}\,\overrightarrow{\delta^{\rho}N}\,\mathrm{in}\,\mathrm{box}\,\overrightarrow{x^{\rho}}\,\mathrm{be}\,\overrightarrow{y}\,\mathrm{in}\,M$$

$$(\mathrm{com}_1)\qquad \delta^{\Box\sigma}(\delta^{\sigma}M) = \mathrm{box}\,x^{\Box\Box\sigma}\,\mathrm{be}\,\delta^{\sigma}M\,\mathrm{in}\,\delta^{\Box\sigma}x$$

$$(\mathrm{com}_2)\qquad \varepsilon^{\Box\sigma}(\delta^{\sigma}M) = \mathrm{box}\,x^{\Box\Box\sigma}\,\mathrm{be}\,\delta^{\sigma}M\,\mathrm{in}\,\varepsilon^{\Box\sigma}x = M$$

Table 6: Axioms for T, K4, and S4

Principles of Programming Languages, pages 47–58. ACM, 1990.

[12] R. Harper, F. Honsell, and G. Plotkin. A framework for defining logics. *Journal of the ACM*, 40(1):143–184, 1993.

[13] W. A. Howard. The formulas-as-types notion of construction. In *Essays on Combinatory Logic, Lambda-Calculus and Formalism*, pages 479–490. Academic Press, 1980.

[14] C. B. Jay. Long $\beta\eta$ normal forms and confluence. LFCS Report ECS-LFCS-91-183, Department of Computer Science, University of Edinburgh, 1991. A revised version is available.

[15] F. Joachimski and R. Matthes. Short proofs of normalization for the simply-typed λ-calculus, permutative conversions and Gödel's T. *Archive for Mathematical Logic*, 42(1):59–87, 2003.

[16] Y. Kakutani. A calculus for classical normal modal logic. Manuscript.

[17] J. Lambek and P. J. Scott. *Introduction to Higher Order Categorical Logic*. Cambridge University Press, 1986.

[18] S. Mac Lane. *Categories for the Working Mathematician*. Springer-Verlag, 2nd edition, 1997.

[19] S. Martini and A. Masini. A computational interpretation of modal proofs. In *Proof Theory of Modal Logics*, pages 213–241. Kluwer, 1994.

[20] G. E. Mints. Theory of categories and theory of proofs (in Russian). In *Urgent Questions of Logic and the Methodology of Science*, 1979.

[21] K. Miyamoto and A. Igarashi. A modal foundation for secure information flow. In *Proceedings of Workshop on Foundations of Computer Security*, pages 187–203, 2004.

[22] M. Parigot. $\lambda\mu$-calculus: an algorithmic interpretation of classical natural deduction. In *Proceedings of International Conference on Logic Programming and Automated Reasoning*, volume 624 of *Lecture Notes in Artificial Intelligence*, pages 190–201. Springer-Verlag, 1992.

[23] F. Pfenning and H.-C. Wong. On a modal lambda calculus for S4. *Electronic Notes in Computer Science*, 1:1–23, 1995.

[24] D. Prawitz. *Natural Deduction*. Almqvist and Wiksell, 1965.

[25] Terese. *Term Rewriting Systems*. Cambridge University Press, 2003.

[26] J. van Benthem. *Correspondence Theory*, volume 2 of *Handbook of Philosophical Logic*, pages 167–247. Reidel, 1984.

Appendix

Proof of Lemma 3.3. By induction on $M \to M'$. In particular, we only refer to a case of a box-term of the length 2, for readability. It is as in Figure 1. The other cases are trivial. ■

Proof of Lemma 3.5. The difference from ordinary λ-calculi is the existence of box-terms. This difference raises new critical pairs. For instance, Figure 2 is a case that both reductions are ones with respect to box-terms. The other cases are left to the reader. ■

$$
\begin{aligned}
[\![\mathrm{box}\ \boxed{\begin{array}{c}x_1\\ x_2\end{array}}\ \mathrm{be}\ \boxed{\begin{array}{c}M_1\\ \mathrm{box}\ y\ \mathrm{be}\ N\ \mathrm{in}\ M_2\end{array}}\ \mathrm{in}\ L]\!] &= \mathrm{case}\ \mathrm{case}[\![N]\!]\ \mathrm{of}\ \frac{y\ \mathrm{in}\ \mathrm{inl}[\![M]\!]}{v\ \mathrm{in}\ \mathrm{inr}\ v}\ \mathrm{of}\ \frac{x_2\ \mathrm{in}\ \mathrm{case}[\![M_1]\!]\ \mathrm{of}\ \dfrac{x_1\ \mathrm{in}\ \mathrm{inl}[\![L]\!]}{w_1\ \mathrm{in}\ \mathrm{inr}\ w_1}}{w_2\ \mathrm{in}\ \mathrm{inr}\ w_2} \\
&\to \mathrm{case}[\![N]\!]\ \mathrm{of}\ \frac{y\ \mathrm{in}\ \mathrm{case}\ \mathrm{inl}[\![M]\!]\ \mathrm{of}\ \dfrac{x_2\ \mathrm{in}\ \mathrm{case}[\![M_1]\!]\ \mathrm{of}\ \dfrac{x_1\ \mathrm{in}\ \mathrm{inl}[\![L]\!]}{w_1\ \mathrm{in}\ \mathrm{inr}\ w_1}}{w_2\ \mathrm{in}\ \mathrm{inr}\ w_2}}{v\ \mathrm{in}\ \mathrm{case}\ \mathrm{inr}\ v\ \mathrm{of}\ \dfrac{x_2\ \mathrm{in}\ \mathrm{case}[\![M_1]\!]\ \mathrm{of}\ \dfrac{x_1\ \mathrm{in}\ \mathrm{inl}[\![L]\!]}{w_1\ \mathrm{in}\ \mathrm{inr}\ w_1}}{w_2\ \mathrm{in}\ \mathrm{inr}\ w_2}} \\
&\to \mathrm{case}[\![N]\!]\ \mathrm{of}\ \frac{y\ \mathrm{in}\ \mathrm{case}[\![M_1]\!]\ \mathrm{of}\ \dfrac{x_1\ \mathrm{in}\ \mathrm{inl}[[\![M]\!]/x_2][\![L]\!]}{w_1\ \mathrm{in}\ \mathrm{inr}\ w_1}}{v\ \mathrm{in}[v/w_2]\ \mathrm{inr}\ w_2} \\
&\equiv \mathrm{case}[\![N]\!]\ \mathrm{of}\ \frac{y\ \mathrm{in}\ \mathrm{case}[\![M_1]\!]\ \mathrm{of}\ \dfrac{x_1\ \mathrm{in}\ \mathrm{inl}[\![[M/x_2]L]\!]}{w_1\ \mathrm{in}\ \mathrm{inr}\ w_1}}{v\ \mathrm{in}\ \mathrm{inr}\ v} \\
&= [\![\mathrm{box}\ \boxed{\begin{array}{c}x_1\\ y\end{array}}\ \mathrm{be}\ \boxed{\begin{array}{c}M_1\\ N\end{array}}\ \mathrm{in}[M_2/x_2]L]\!]
\end{aligned}
$$

Figure 1: Preservation of a reduction of box-terms

$$
\begin{array}{ccc}
 & \mathrm{box}\ x^{\rho}\ \mathrm{be}\ \mathrm{box}\ y^{\sigma}\ \mathrm{be}\ \mathrm{box}\ z^{\tau}\ \mathrm{be}\ N\ \mathrm{in}\ M\ \mathrm{in}\ L\ \mathrm{in}\ K & \\
\swarrow & & \searrow \\
\mathrm{box}\ y^{\sigma}\ \mathrm{be}\ \mathrm{box}\ z^{\tau}\ \mathrm{be}\ N\ \mathrm{in}\ M\ \mathrm{in}[L/x]K & & \mathrm{box}\ x^{\rho}\ \mathrm{be}\ \mathrm{box}\ z^{\tau}\ \mathrm{be}\ N\ \mathrm{in}[M/y]L\ \mathrm{in}\ K \\
\downarrow & & \downarrow \\
 & \mathrm{box}\ z^{\tau}\ \mathrm{be}\ N\ \mathrm{in}[M/y][L/x]K \equiv \mathrm{box}\ z^{\tau}\ \mathrm{be}\ N\ \mathrm{in}[[M/y]L/x]K &
\end{array}
$$

Figure 2: Confluence of a critical pair