Constructive Linear-Time Temporal Logic: Proof Systems and Kripke Semantics

Kensuke Kojima, Atsushi Igarashi

Graduate School of Informatics
Kyoto University
Kyoto, Japan

Abstract

In this paper we study a version of constructive linear-time temporal logic (LTL) with the "next" temporal operator. The logic is originally due to Davies, who has shown that the proof system of the logic corresponds to a type system for binding-time analysis via the Curry-Howard isomorphism. However, he did not investigate the logic itself in detail; he has proved only that the logic augmented with negation and classical reasoning is equivalent to (the "next" fragment of) the standard formulation of classical linear-time temporal logic. We give natural deduction, sequent calculus and Hilbert-style proof systems for constructive LTL with conjunction, disjunction and falsehood, and show that the sequent calculus enjoys cut elimination. Moreover, we also consider Kripke semantics and prove soundness and completeness. One distinguishing feature of this logic is that distributivity of the "next" operator over disjunction "$\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$" is rejected in view of a type-theoretic interpretation.

Key words: constructive linear-time temporal logic, Kripke semantics, sequent calculus, cut elimination

1. Introduction

Temporal logic is a family of (modal) logics in which the truth of propositions depends on time, and is useful to describe various properties of state transition systems. Linear-time temporal logic (LTL, for short), which is used to reason about properties of a fixed execution path of a state transition system, is temporal logic in which each time has a unique time that follows it.

In this paper, we study a constructive propositional LTL with only the "next" temporal operator $\bigcirc$. Our contributions are (1) to give natural deduction, sequent calculus (satisfying cut elimination), and Hilbert-style proof

Email addresses: kozima@kuis.kyoto-u.ac.jp (Kensuke Kojima), igarashi@kuis.kyoto-u.ac.jp (Atsushi Igarashi)

systems and (2) to give Kripke-style semantics together with completeness theorem.

Intuitionistic versions of LTL have been already considered in the literature [1, 2]. However, a characteristic feature of our version of LTL is that the "distributivity law" $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$, is *not* admitted in our logic, while (to our knowledge) it is admitted in the other formalizations as well as in the classical setting.

The motivation not to admit the distributivity law above comes from the type-theoretic interpretation of $\bigcirc$ operator, first given by Davies [3]. He pointed out that a proof system of LTL can be related to a type system of (multi-level) binding-time analysis, which is used in offline partial evaluation [4] to determine which part of a program can be computed at specialization-time and which is residualized. According to this correspondence, a formula $\bigcirc A$, which means that A holds at the next time, is interpreted as a type of (residual) *code* of type A; introduction and elimination rules of $\bigcirc$ are as Lisp-like quasiquotation and unquote, respectively. As a result, $\lambda^{\bigcirc}$ terms can be considered as program-generating programs, such as parser generators or generating extensions, which manipulate code fragments by the quasiquotation mechanism. For example, a parser generator would have a type like `parser_spec` → $\bigcirc$(`string` → `syntax_tree`). Now, a proof of the distributivity law would be considered a function which takes a value of type $\bigcirc(A \vee B)$ and returns a value of type $\bigcirc A \vee \bigcirc B$. While a value of the return type must be of type $\bigcirc A$ or type $\bigcirc B$ with a tag indicating which of the two is actually the case, a value of the argument type is *quoted* code, which will not be executed *until the next time comes*, that is, until the residual code is executed; it is in general impossible to know which value (A or B) this code evaluates to *now* (unless a Lisp-like eval function was available). From this observation, we conclude that there is no method to turn a value of type $\bigcirc(A \vee B)$ into a value of type $\bigcirc A \vee \bigcirc B$, and hence $\bigcirc A \vee \bigcirc B$ should be strictly stronger than $\bigcirc(A \vee B)$.

Similarly, we also reject $\bigcirc\bot \supset \bot$, which is admitted in classical LTL. The falsehood $\bot$ is interpreted as a type which has no value, so a program of type $\bot$ does not terminate normally. However, a program of type $\bigcirc\bot$ will terminate normally, although the resulting value (which is code of type $\bot$) would not, when executed.

Davies defined a natural deduction system for a constructive LTL with only the "next" operator $\bigcirc$ and implication, and derived via the Curry-Howard isomorphism a typed λ-calculus $\lambda^{\bigcirc}$, which was formally shown to be equivalent to a type system of multi-level binding-time analysis by Glück and Jørgensen [5]. Unfortunately, however, Davies did not investigate his system in detail, from a logical point of view: he proved only that his system augmented with negation and classical reasoning is equivalent to the *classical* LTL, even though the logic can be considered a *constructive* version of LTL. The main aim of this paper is to see how his system is formalized in terms of Kripke semantics and sequent calculus. Davies' original system is an implicational fragment, but we also consider other connectives.[1]

This paper is an extended version of the authors' previous work [6]. In addition to the previous version, this paper considers (1) falsehood in our logic, (2) more concise Kripke semantics, and (3) some discussions on informal interpretation of the semantics we give.

The organization of the rest of this paper is as follows. In Section 2, we discuss the natural-deduction proof system. We first review the system by Davies, and extend it with conjunction, disjunction and falsehood. In Section 3 we define a sequent calculus $\mathrm{LJ}^{\bigcirc}$, which is equivalent to the natural deduction, with its cut elimination procedure. In Section 4 we show Hilbert-style proof system which is equivalent to the natural deduction given in Section 2. Section 5 considers Kripke semantics. It turns out that, although our logic is considered to be a version of LTL, a straightforward extension of classical semantics is not suitable for our interpretation of $\bigcirc$. After seeing that, we consider another Kripke semantics and establish soundness and completeness of the proof system. Finally, we give concluding remarks in Section 6.

2. Natural Deduction

In this section, we first recall the natural deduction system by Davies and some of its properties, and then extend the system with conjunction, disjunction and falsehood.

2.1. Results by Davies

The temporal logic Davies considered contains only $\bigcirc$ ("next" operator) and $\supset$ (intuitionistic implication). So here we consider formulas containing only these two connectives.

A judgment in his system takes the form

$$A_1^{n_1}, \ldots, A_k^{n_k} \vdash B^m$$

where A_i, B are formulas and n_i, m are natural numbers; it is read "B holds at time m under the assumption that A_i holds at time n_i (for $i = 1, \ldots, k$)." In what follows, we use A, B, C, D for formulas, k, l, m, n for natural numbers, F, G for annotated formulas (i.e. formulas with time annotation), and Γ, Δ for sets of annotated formulas. We consider the left-hand side of a judgment a set.

Inference rules of Davies' system are listed in Figure 1. The rules $\supset$I, $\supset$E, and Axiom are standard. The other two, the introduction and elimination rules for $\bigcirc$ operator, state that A holds at time $n+1$ if and only if $\bigcirc A$ holds at time n. This is quite natural since $\bigcirc A$ means that "A holds at the next time."

To show that $\bigcirc$ operator in this system is indeed the "next" operator in linear-time temporal logic, Davies compared his system with $L^{\bigcirc}$, a well-known

[1] Precisely speaking, Davies extended $\lambda^{\bigcirc}$ with pairing and natural numbers, but did not consider conjunction or disjunction in his logic.

$$\frac{}{\Gamma, A^n \vdash A^n}\ (\text{Axiom}) \qquad \frac{\Gamma, A^n \vdash B^n}{\Gamma \vdash A \supset B^n}\ (\supset\text{I})$$

$$\frac{\Gamma \vdash A \supset B^n \qquad \Gamma \vdash A^n}{\Gamma \vdash B^n}\ (\supset\text{E}) \qquad \frac{\Gamma \vdash A^{n+1}}{\Gamma \vdash \bigcirc A^n}\ (\bigcirc\text{I})$$

$$\frac{\Gamma \vdash \bigcirc A^n}{\Gamma \vdash A^{n+1}}\ (\bigcirc\text{E})$$

Figure 1: Derivation Rules of Davies' System.

$$\frac{\Gamma \vdash A \wedge B^n}{\Gamma \vdash A^n}\ (\wedge\text{E1}) \qquad \frac{\Gamma \vdash A^n \qquad \Gamma \vdash B^n}{\Gamma \vdash A \wedge B^n}\ (\wedge\text{I})$$

$$\frac{\Gamma \vdash A \wedge B^n}{\Gamma \vdash B^n}\ (\wedge\text{E2}) \qquad \frac{\Gamma \vdash A^n}{\Gamma \vdash A \vee B^n}\ (\vee\text{I1})$$

$$\frac{\Gamma \vdash A \vee B^n \qquad \Gamma, A^n \vdash C^n \qquad \Gamma, B^n \vdash C^n}{\Gamma \vdash C^n}\ (\vee\text{E}) \qquad \frac{\Gamma \vdash B^n}{\Gamma \vdash A \vee B^n}\ (\vee\text{I2})$$

$$\frac{\Gamma \vdash \bot^n}{\Gamma \vdash A^n}\ (\bot\text{E})$$

Figure 2: Additional Rules for Full NJ$^{\bigcirc}$.

Hilbert-style proof system of the fragment of classical linear-time temporal logic consisting of only implication, negation and next operators. The axiomatization is given by Stirling, who also proved that $L^{\bigcirc}$ is sound and complete for the standard semantics [7]. The axioms and rules of $L^{\bigcirc}$ are as follows:

Axioms • any classical tautology instance

- $\bigcirc\neg A \supset \neg\bigcirc A$
- $\neg\bigcirc A \supset \bigcirc\neg A$
- $\bigcirc(A \supset B) \supset \bigcirc A \supset \bigcirc B$

Rules • if $A \supset B$ and A then B

- if A then $\bigcirc A$

Davies proved that his system extended by negation and classical reasoning is equivalent to $L^{\bigcirc}$ in the following sense [3]:

Proposition 1. *A judgment $A_1^{n_1}, \ldots, A_k^{n_k} \vdash B^m$ is provable in the extended system if and only if $\bigcirc^{n_1} A_1 \supset \ldots \supset \bigcirc^{n_k} A_k \supset \bigcirc^m B$ has a proof in $L^{\bigcirc}$. In particular, $\cdot \vdash A^0$ is provable if and only if A is a theorem of $L^{\bigcirc}$.*

2.2. Full System

Next we extend Davies' system with conjunction, disjunction and falsehood. We call the extended system NJ$^{\bigcirc}$. Additional derivation rules are listed in Figure 2. The rules for conjunction and introduction rules for disjunction are fairly straightforward, but the other two rules would require some explanation.

In $\vee$E, the formula being eliminated must have the same time as the succedent of the conclusion. At first sight it may seem strange, but in fact this restriction is essential for our system. Indeed, without this restriction we could prove the distributivity law $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$, which should not be a tautology as mentioned above, as follows:

$$\dfrac{\dfrac{\bigcirc(A \vee B)^0 \vdash \bigcirc(A \vee B)^0}{\bigcirc(A \vee B)^0 \vdash A \vee B^1} \quad \dfrac{\dfrac{\bigcirc(A \vee B)^0, A^1 \vdash A^1}{\bigcirc(A \vee B)^0, A^1 \vdash \bigcirc A^0}}{\bigcirc(A \vee B)^0, A^1 \vdash \bigcirc A \vee \bigcirc B^0} \quad \dfrac{\dfrac{\bigcirc(A \vee B)^0, B^1 \vdash B^1}{\bigcirc(A \vee B)^0, B^1 \vdash \bigcirc B^0}}{\bigcirc(A \vee B)^0, A^1 \vdash \bigcirc A \vee \bigcirc B^0}}{\bigcirc(A \vee B)^0 \vdash \bigcirc A \vee \bigcirc B^0}\ \vee\mathrm{E}$$

In this proof, disjunction being eliminated has time 1 while the time of the succedent is 0.

For the same reason, we needed to restrict the time of A in $\bot$E to be the same as the time of $\bot$ being eliminated. Otherwise, $\bigcirc\bot \supset \bot$ would be a theorem.

In fact, the problem would occur only if we allowed the time of the succedent to be strictly less than that of the formula being eliminated. A slight variation of $\vee$E in which C^n is changed to C^m with the side condition $m \geq n$ is provable by using $\bigcirc$I and $\bigcirc$E. In the same way, a variant of $\bot$E which derives A^m from $\bot^n$ for $m \geq n$ is also provable.

3. Sequent Calculus

In this section we give another formalization $\mathrm{LJ}^{\bigcirc}$ of our logic in the sequent calculus style. After verifying that the system $\mathrm{LJ}^{\bigcirc}$ is equivalent to $\mathrm{NJ}^{\bigcirc}$ previously defined, we give a cut-elimination procedure for $\mathrm{LJ}^{\bigcirc}$.

3.1. Formalization

Sequents of $\mathrm{LJ}^{\bigcirc}$ have the form $\Gamma \Rightarrow F$ where Γ is a set of annotated formulas and F is an annotated formula. Inference rules of $\mathrm{LJ}^{\bigcirc}$ are listed in Figure 3.

Since we regard the left-hand side of a sequent as a set, exchange and contraction rules are not explicitly included. There is not an explicit weakening rule, either—we included weakening implicitly by allowing extra formulas in the rules Init and $\bot$L. Most of the rules are standard, but we comment on some rules. In rules Init and $\bot$L, we restricted the right-hand side to be atomic to make the proof of cut elimination theorem simpler (but this does not reduce the proof-theoretic strength). In rules $\bot$L and $\vee$L, the time of the succedent must be no less than that of the principal formula ($\bot$ and $A \vee B$, respectively). This corresponds to the issue mentioned in Section 2 that we cannot eliminate falsehood or disjunction with a succedent of an earlier time.

$\mathrm{LJ}^{\bigcirc}$ is equivalent to $\mathrm{NJ}^{\bigcirc}$ in the following sense:

Theorem 2. *A sequent* $\Gamma \Rightarrow F$ *is provable in* $\mathrm{LJ}^{\bigcirc}$ *if and only if* $\Gamma \vdash F$ *is provable in* $\mathrm{NJ}^{\bigcirc}$.

To prove this, it is sufficient to check that all rules of $\mathrm{LJ}^{\bigcirc}$ are admissible in $\mathrm{NJ}^{\bigcirc}$ and vice versa. For the former part we need the admissibility of weakening and cut in natural deduction:

$$\dfrac{(A \text{ is atomic})}{\Gamma, A^n \Rightarrow A^n}\ (\text{Init}) \qquad \dfrac{\Gamma \Rightarrow F \qquad F, \Delta \Rightarrow G}{\Gamma, \Delta \Rightarrow G}\ (\text{Cut})$$

$$\dfrac{\Gamma \Rightarrow A^n \qquad \Gamma, B^n \Rightarrow F}{\Gamma, A \supset B^n \Rightarrow F}\ (\supset\text{L}) \qquad \dfrac{\Gamma, A^n \Rightarrow B^n}{\Gamma \Rightarrow A \supset B^n}\ (\supset\text{R})$$

$$\dfrac{\Gamma, A^n \Rightarrow F}{\Gamma, A \wedge B^n \Rightarrow F}\ (\wedge\text{L1}) \qquad \dfrac{\Gamma \Rightarrow A^n \qquad \Gamma \Rightarrow B^n}{\Gamma \Rightarrow A \wedge B^n}\ (\wedge\text{R})$$

$$\dfrac{\Gamma, B^n \Rightarrow F}{\Gamma, A \wedge B^n \Rightarrow F}\ (\wedge\text{L2}) \qquad \dfrac{\Gamma \Rightarrow A^n}{\Gamma \Rightarrow A \vee B^n}\ (\vee\text{R1})$$

$$\dfrac{\Gamma, A^n \Rightarrow C^{n+m} \qquad \Gamma, B^n \Rightarrow C^{n+m}}{\Gamma, A \vee B^n \Rightarrow C^{n+m}}\ (\vee\text{L}) \qquad \dfrac{\Gamma \Rightarrow B^n}{\Gamma \Rightarrow A \vee B^n}\ (\vee\text{R2})$$

$$\dfrac{\Gamma, A^{n+1} \Rightarrow F}{\Gamma, \bigcirc A^n \Rightarrow F}\ (\bigcirc\text{L}) \qquad \dfrac{\Gamma \Rightarrow A^{n+1}}{\Gamma \Rightarrow \bigcirc A^n}\ (\bigcirc\text{R})$$

$$\dfrac{(A \text{ is atomic})}{\Gamma, \bot^n \Rightarrow A^{n+m}}\ (\bot\text{L})$$

Figure 3: Inference Rules of LJ$^{\bigcirc}$.

Lemma 3. 1. *If* $\Gamma \vdash F$ *is provable, then* $\Gamma, \Delta \vdash F$ *is also provable.*

2. *If* $\Gamma \vdash F$ *and* $F, \Delta \vdash G$ *are provable, then* $\Gamma, \Delta \vdash G$ *is also provable.*

Then, both directions are proved by easy induction, so we omit the details.

3.2. Cut Elimination Procedure

Next we show that cut is admissible in the cut-free fragment of LJ$^{\bigcirc}$.

Theorem 4. *If* $\Gamma \Rightarrow F$ *and* $F, \Delta \Rightarrow G$ *are provable without cut, then* $\Gamma, \Delta \Rightarrow G$ *is also provable without cut.*

We sketch the proof below. Consider the cut

$$\dfrac{\mathcal{D}_1 = \dfrac{\vdots}{\Gamma \Rightarrow F}\ R_1 \qquad \mathcal{D}_2 = \dfrac{\vdots}{F, \Delta \Rightarrow G}\ R_2}{\Gamma, \Delta \Rightarrow G}\ \text{Cut}$$

We split this into five cases:

1. R_1 is neither $\vee$L nor $\bot$L, or $R_2 = \text{Init}$;
2. F is not principal in $\mathcal{D}_2$;
3. $R_1 = \bot$L and F is principal in $\mathcal{D}_2$;
4. $R_1 = \vee$L, R_2 is either $\vee$L or $\bot$L, and F is principal in $\mathcal{D}_2$;
5. $R_1 = \vee$L, F is principal in $\mathcal{D}_2$, and F is neither atomic nor disjunction.

The standard cut-elimination procedure works in case 1, but in the other cases, it is not as obvious. The problem stems from the side condition on the time on the principal formula and that on the succedent in $\vee$L. Consider the most general form of cut with $R_1 = \vee$L:

$$\dfrac{\dfrac{\Gamma, A^n \Rightarrow C^m \quad \Gamma, B^n \Rightarrow C^m}{\Gamma, A \vee B^n \Rightarrow C^m}\,\vee\mathrm{L} \qquad C^m, \Delta \Rightarrow D^l}{\Gamma, A \vee B^n, \Delta \Rightarrow D^l}\,\mathrm{Cut}$$

Applying the standard procedure to this derivation, we would obtain a new derivation

$$\dfrac{\dfrac{\Gamma, A^n \Rightarrow C^m \quad C^m, \Delta \Rightarrow D^l}{\Gamma, A^n, \Delta \Rightarrow D^l}\,\mathrm{Cut} \qquad \dfrac{\Gamma, B^n \Rightarrow C^m \quad C^m, \Delta \Rightarrow D^l}{\Gamma, B^n, \Delta \Rightarrow D^l}\,\mathrm{Cut}}{\Gamma, A \vee B^n, \Delta \Rightarrow D^l}\,\vee\mathrm{L}$$

which, however, is not always valid, because it is not necessarily the case that $l \geq n$. So, we split this case into the three subcases 2–5 listed above.

In case 2 it is easy to reduce the cut into a simpler one: as the cut formula is not principal in $\mathcal{D}_2$, it occurs in all premises of R_2, so we just lift the cut into $\mathcal{D}_2$. For example, if $R_2 = \bigcirc$L we proceed

$$\dfrac{\Gamma \Rightarrow F \qquad \dfrac{F, \Delta', A^{n+1} \Rightarrow G}{F, \Delta', \bigcirc A^n \Rightarrow G}\,\bigcirc\mathrm{L}}{\Gamma, \Delta', \bigcirc A^n \Rightarrow G}\,\mathrm{Cut} \quad \Longrightarrow \quad \dfrac{\dfrac{\Gamma \Rightarrow F \quad F, \Delta', A^{n+1} \Rightarrow G}{\Gamma, \Delta', A^{n+1} \Rightarrow G}\,\mathrm{Cut}}{\Gamma, \Delta', \bigcirc A^n \Rightarrow G}\,\bigcirc\mathrm{L}$$

Next, consider the case 3. If $R_2 = \bot$L, the cut has the from

$$\dfrac{\Gamma, \bot^n \Rightarrow \bot^m \quad \bot^m, \Delta \Rightarrow A^l}{\Gamma, \bot^n, \Delta \Rightarrow A^l}\,\mathrm{Cut}$$

where $n \leq m \leq l$. In this case the conclusion can be derived directly by using $\bot$L because the side condition $n \leq l$ is met. If $R_2 \neq \bot$L, then there exists a subformula B of A such that the cut has the form

$$\dfrac{\Gamma, \bot^n \Rightarrow A^m \qquad \dfrac{\cdots \quad B^l, \Delta \Rightarrow G}{A^m, \Delta \Rightarrow G}}{\Gamma, \bot^n, \Delta \Rightarrow G}\,\mathrm{Cut}$$

where $n \leq m$, and $l = m + 1$ if $R_2 = \bigcirc$L and $l = m$ otherwise. In any case we have $n \leq l$, so we can cut B^l instead of A^m as follows:

$$\dfrac{\Gamma, \bot^n \Rightarrow B^l \quad B^l, \Delta \Rightarrow G}{\Gamma, \bot^n, \Delta \Rightarrow G}\,\mathrm{Cut}$$

In case 4, we can use the standard procedure above because the condition $n \leq l$ is always met. Indeed, if both R_1 and R_2 are $\vee$L, $\mathcal{D}_1$ and $\mathcal{D}_2$ have the form

$$\mathcal{D}_1 = \dfrac{\Gamma, A^n \Rightarrow C_1 \vee {C_2}^m \quad \Gamma, B^n \Rightarrow C_1 \vee {C_2}^m}{\Gamma, A \vee B^n \Rightarrow C_1 \vee {C_2}^m}\,\vee\mathrm{L}$$

$$\mathcal{D}_2 = \dfrac{C_1^m, \Delta \Rightarrow D^l \quad C_2^m, \Delta \Rightarrow D^l}{C_1 \vee {C_2}^m, \Delta \Rightarrow D^l}\,\vee\mathrm{L}$$

and we have $n \leq m$ and $m \leq l$ from the side condition of $\vee$L. When $R_2 = \bot$L, we can check $n \leq l$ in the same way.

The last case is the case 5, in which F is neither atomic nor disjunction. In this case, first rewrite a given derivation $\mathcal{D}_1$ into another derivation $\mathcal{D}'_1$ of the same sequent such that the new derivation ends with the application of a right rule. Then, the given cut becomes a principal cut, which is easily reduced into a simpler cut. To do this, all we need is the following lemma:

Lemma 5. *If a sequent $S \equiv \Gamma \Rightarrow F$ has a cut-free derivation $\mathcal{D}$ and F is neither atomic formula nor disjunction, then there exists a cut-free derivation $\mathcal{D}'$ of S such that the last rule used in $\mathcal{D}'$ is a right rule.*

Proof. It is sufficient to show that any use of a left rule immediately following a right rule other than the $\vee$-right rules can be replaced by applications of the right rule following the left rule. Intuitively this means that by a conversion like

$$\dfrac{\dfrac{T_1 \quad \dots \quad T_k}{S'}\,\text{Right}}{S}\,\text{Left} \quad\Longrightarrow\quad \dfrac{\dfrac{T_1}{S'_1}\,\text{Left} \quad \dots \quad \dfrac{T_k}{S'_k}\,\text{Left}}{S}\,\text{Right}$$

we always obtain a valid derivation from a valid derivation. This is because, from the assumption that F is neither atomic nor disjunction, a right rule which derives $\Gamma \Rightarrow F$ is uniquely determined (this fact is used when lifting $\vee$L rule).

The actual proof is done by straightforward case analysis. For example, if the left rule is $\supset$L and the right rule is $\supset$R, then

$$\dfrac{\Gamma \Rightarrow A^n \quad \dfrac{\Gamma, B^n, C^m \Rightarrow D^m}{\Gamma, B^n \Rightarrow C \supset D^m}\,\supset\!\text{R}}{\Gamma, A \supset B^n \Rightarrow C \supset D^m}\,\supset\!\text{L} \quad\Longrightarrow\quad \dfrac{\dfrac{\Gamma \Rightarrow A^n \quad \Gamma, B^n, C^m \Rightarrow D^m}{\Gamma, A \supset B^n, C^m \Rightarrow D^m}\,\supset\!\text{L}}{\Gamma, A \supset B^n \Rightarrow C \supset D^m}\,\supset\!\text{R}$$

and for $\vee$L and $\bigcirc$R we have

$$\dfrac{\dfrac{\Gamma, A^n \Rightarrow C^{m+1}}{\Gamma, A^n \Rightarrow \bigcirc C^m}\,\bigcirc\text{R} \quad \dfrac{\Gamma, B^n \Rightarrow C^{m+1}}{\Gamma, B^n \Rightarrow \bigcirc C^m}\,\bigcirc\text{R} \quad (m \geq n)}{\Gamma, A \vee B^n \Rightarrow \bigcirc C^m}\,\vee\text{L}$$

$$\Longrightarrow \quad \dfrac{\dfrac{\Gamma, A^n \Rightarrow C^{m+1} \quad \Gamma, B^n \Rightarrow C^{m+1} \quad (m+1 \geq n)}{\Gamma, A \vee B^n \Rightarrow C^{m+1}}\,\vee\text{L}}{\Gamma, A \vee B^n \Rightarrow \bigcirc C^m}\,\bigcirc\text{R}$$

Other cases are similar.

From the argument above, we obtain the cut-elimination theorem for LJ$^{\bigcirc}$.

Theorem 6. *If a sequent is provable in* LJ$^{\bigcirc}$*, then it has a cut-free proof.*

The following is an easy consequence of cut-elimination theorem and equivalence of LJ$^{\bigcirc}$ and NJ$^{\bigcirc}$.

Theorem 7. *In neither* LJ$^{\bigcirc}$ *nor* NJ$^{\bigcirc}$ *the distributivity law $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$ is provable, as well as $\bigcirc\bot \supset \bot$.*

This result shows that our systems indeed have an intended property of rejecting these laws.

4. Hilbert-Style Axiomatization

Next we briefly describe how the logic defined above is characterized in the Hilbert-style. Interestingly, there exists a quite simple axiomatization.

Proposition 8. *Consider the proof system given by the following sets of axioms and rules.*

Axioms

- *any intuitionistic tautology instance*
- $\bigcirc(A \supset B) \supset \bigcirc A \supset \bigcirc B$
- $(\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)$

Rules

- *if* $A \supset B$ *and* A *then* B
- *if* A *then* $\bigcirc A$

Then, this system is equivalent to $\mathrm{NJ}^{\bigcirc}$ *in the same sense as the Proposition 1.*

Therefore we can say that our logic, formalized as $\mathrm{NJ}^{\bigcirc}$ in Section 2, is obtained by adding axiom $(\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)$, which we call **CK** as it is the "converse" of the axiom **K**, to the minimal normal intuitionistic modal logic (with only $\Box$ modality).

The axiomatization above (in particular, the axiom **CK**) is due to Yuse and Igarashi [8]. They extended Davies' natural deduction system and $\lambda^{\bigcirc}$ with $\Box$ operator, which is similar to "always" operator in classical LTL, and conjectured that their Hilbert-style system and natural deduction system are equivalent. The axiomatization above is its $\Box$-free fragment.

Below we are going to sketch the proof. First, we show that the axioms and rules are sound with respect to $\mathrm{NJ}^{\bigcirc}$. The axiom **CK** is the only non-standard clause, so we only check this axiom. Provability of **CK** is easily seen from the following derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\bigcirc A \supset \bigcirc B^0, A^1 \vdash \bigcirc A \supset \bigcirc B^0 \qquad \dfrac{\bigcirc A \supset \bigcirc B^0, A^1 \vdash A^1}{\bigcirc A \supset \bigcirc B^0, A^1 \vdash \bigcirc A^0}\,\bigcirc\mathrm{I}}{\bigcirc A \supset \bigcirc B^0, A^1 \vdash \bigcirc B^0}\,{\supset}\mathrm{E}}{\bigcirc A \supset \bigcirc B^0, A^1 \vdash B^1}\,\bigcirc\mathrm{E}}{\bigcirc A \supset \bigcirc B^0 \vdash A \supset B^1}\,{\supset}\mathrm{I}}{\bigcirc A \supset \bigcirc B^0 \vdash \bigcirc(A \supset B)^0}\,\bigcirc\mathrm{I}}{\cdot \vdash (\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)^0}\,{\supset}\mathrm{I}$$

For the converse, we only mention the admissibility of $\supset$I, which is the most essential part (actually $\vee$E is also nontrivial, but can be checked in a similar way). Putting Γ aside, this rule says that "if $A^n \vdash B^n$, then $\cdot \vdash A^n \supset B^n$." To prove this rule is admissible, it is sufficient to show that "if $\bigcirc^n A \supset \bigcirc^n B$, then $\bigcirc^n(A \supset B)$," and this is an immediate consequence of the axiom **CK**.

5. Kripke Semantics

In this section, we consider Kripke semantics for the logic defined above, and establish soundness and completeness for that semantics.

First, let us briefly review existing approaches upon which our study is based. Classically, semantics of modal logic is typically given by using relational structures (Kripke frames). In the intuitionistic setting, its analogues are commonly used in the literature ([2, 9, 10, 11, 12, 13], for example). Following one of the existing approaches, we consider so-called birelational Kripke frames. They consist of a set of possible worlds together with two accessibility relations R and $\leq$. These two relations are taken from classical modal logic and intuitionistic logic, respectively, and therefore $\leq$ is assumed to be a partial order.

Before the technical details, we sketch the rest of this section. First we mention that classical LTL can be described in terms of Kripke frames whose accessibility relation is a function. From this fact it seems natural to consider a semantics based on birelational semantics whose modal accessibility is a function. Unfortunately, however, exploiting this condition turns out that the resulting semantics admits the distributivity law, which we need to avoid. After seeing that, we examine an already known class of birelational frames, IM-frames [12]. We can give a class of IM-frames which corresponds to our logic by identifying the corresponding frame condition. This approach works well in the sense that it establishes a semantics for which soundness and completeness hold, but it is not satisfactory for us since linearity of time has been lost. Moreover, it seems difficult to tell intuitive meanings of the frame condition. For this reason, we consider deriving another version from this semantics, by decomposing modal accessibility relation of IM-frames (actually, this decomposition process appears implicitly in the proof of completeness). This gives another class of birelational frames whose modal accessibility is a partial function with some properties. As a result we obtain an equivalent, but more comprehensible representation of IM-frame semantics for our logic. Finally we make some comments on the intuitive meaning of frame conditions.

5.1. Functional Kripke Frames

In this subsection, we are going to examine a class of birelational Kripke frames which comes from the semantics of classical LTL in a fairly straightforward manner. Although this semantics seems natural, and works well for the implicational fragment, it turns out that it admits distributivity law which we reject.

Consider Kripke frames whose accessibility relation R on possible worlds is a function. We say such a frame is *functional*. The term "functional frame" is, to our knowledge, first used by Segerberg [14] (to be precise, he used the terminology "totally functional frames" to mean functional frames in our terminology), but not in context of semantics of LTL. This condition implies that, in a functional Kripke frame, the next state of a given state is uniquely determined, hence justifying "linear time." Although the semantics of classical LTL is often given by using execution paths of transition systems, it is easy to translate it into Kripke-style semantics using functional frames.

Now, let us consider functional frames augmented by intuitionistic accessibility relation $\leq$.

Definition 9. An *intuitionistic functional frame* is a triple $\langle W, \leq, R\rangle$ of a nonempty set W, a partial order $\leq$ on W and a function R from W to W such that $(\leq ; R) = (R ; \leq)$ holds. Here $(\cdot ; \cdot)$ stands for the composition of binary relations defined by $x \ (R ; S) \ y \iff \exists z.(x \ R \ z \ S \ y)$, regarding a function as a special case of binary relations.

Hereafter, we simply say functional frame when no confusion arises.

Using functional frames we can define a satisfaction relation on formulas.

Definition 10. Let $\langle W, \leq, R\rangle$ be a functional frame and $\Vdash$ be a binary relation between W and the set of propositional variables such that $w \leq w'$ and $w \Vdash p$ imply $w' \Vdash p$. Then we can extend $\Vdash$ to formulas by induction with

- $w \Vdash A \supset B \iff$ if $w \leq w'$ and $w' \Vdash A$ then $w' \Vdash B$;
- $w \Vdash A \vee B \iff w \Vdash A$ or $w \Vdash B$;
- $w \Vdash A \wedge B \iff w \Vdash A$ and $w \Vdash B$;
- $w \Vdash \bot$ never occurs;
- $w \Vdash \bigcirc A \iff$ if $w \ R \ w'$ then $w' \Vdash A$.

We also write $w \Vdash A^n$ for $w \Vdash \bigcirc^n A$.

As is easily verified by induction on the construction of formulas, this semantics satisfies the heredity condition.

Lemma 11. *If $w \leq w'$ and $w \Vdash A$, then $w' \Vdash A$.*

It is not very difficult to see that soundness and completeness hold for $\vee, \bot$-free fragment. Soundness is proved by straightforward induction on the derivation. Completeness is proved by the canonical model technique, which is sketched below.

For a set T of formulas, we write $\bigcirc^{-1}T$ for the set $\{A \mid \bigcirc A \in T\}$ and $\bigcirc T$ for $\{\bigcirc A \mid A \in T\}$. Take the set of all theories (of $\vee, \bot$-free fragment) as W, let $\leq$ be a set-inclusion, and R the function which sends each theory T to the theory $\bigcirc^{-1}T$. Then we can show that this defines a functional frame, and if we define $\Vdash$ to be the satisfaction relation such that $T \Vdash p \iff p \in T$, it holds that $T \Vdash A \iff A \in T$ for each formula A, as usual. Finally, if $\Gamma \vdash A^n$ is not provable, take the set $\left\{A \,\middle|\, \Gamma \vdash A^0\right\}$ as T. Then $T \Vdash \Gamma$ holds but $T \Vdash A^n$ does not.

The proof strategy above is almost standard, but notice that we took the set of all theories as W, instead of taking only prime theories. When we consider disjunction and falsehood, the same method will not work. In fact, functional frames are not appropriate in the presence of these connectives, because they validate the laws $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$ and $\bigcirc\bot \supset \bot$, which we reject. It does not seem easy to adjust the definition of the satisfaction relation to exclude them without relaxing the functionality condition.

In the next subsection, we put functionality aside and consider a large class of frames, and try to find its subclass corresponding to the intended logic.

5.2. Semantics Based on IM-frames

As we have mentioned after Theorem 7, the logic defined by $\mathrm{NJ}^{\bigcirc}$ (or other proof systems defined above) is an appropriate one from our motivation. So the reason why completeness for the full system fails is that the choice of functional frame was incorrect. Therefore the next question is what kind of frames correspond to our logic.

The first answer we give is $\mathrm{IM}^{\bigcirc}$-frames defined below.

Definition 12.

1. Let W be a nonempty set, $\leq$ a partial order on W, and R a binary relation on W. We call the triple $\langle W, \leq, R\rangle$ an *IM-frame* if it satisfies $(\leq ; R ; \leq) = R$.
2. An $\mathrm{IM}^{\bigcirc}$*-frame* is an IM-frame $\langle W, \leq, R\rangle$ satisfying the condition: if $w \; R \; v$, then there exists w' such that $w \leq w'$ and $\forall u \in W.(w' \; R \; u \iff v \leq u)$.

Note that, in the definition of $\mathrm{IM}^{\bigcirc}$-frame above, R is not assumed to be a function.

The satisfaction relation is defined in the same way as the functional frame semantics, and heredity is also verified easily.

Theorem 13 (Soundness). *Suppose that* $\Gamma \vdash A^n$ *is provable in* $\mathrm{NJ}^{\bigcirc}$*. Then for any* $\mathrm{IM}^{\bigcirc}$*-frame* $\langle W, \leq, R\rangle$*, satisfaction relation* $\Vdash$*, and possible world* $w \in W$ *such that* $w \Vdash \Gamma$*, it holds that* $w \Vdash A^n$*.*

Proof. Induction on the derivation.

Theorem 14 (Completeness). *If* $w \Vdash \Gamma$ *implies* $w \Vdash A^n$ *for any* $\mathrm{IM}^{\bigcirc}$*-frame* $\langle W, \leq, R\rangle$*, satisfaction relation* $\Vdash$*, and possible world* $w \in W$*, then there exists a derivation of* $\Gamma \vdash A^n$*.*

To prove this, we use the canonical model construction. The canonical Kripke frame is defined in the usual way:

Definition 15.

1. A set of formulas T is said to be a theory if it is deductively closed (if A is provable from T then $A \in T$) and consistent ($\bot \notin T$).
2. A theory T is said to be prime if $A \vee B \in T$ implies either $A \in T$ or $B \in T$.
3. The canonical Kripke frame is the triple $\langle W, \leq, R\rangle$ such that W is the set of prime theories, $\leq$ the set-inclusion on W, and R the relation defined by: $T \; R \; T' \iff \bigcirc^{-1}T \subseteq T'$.

Then, as usual, it is easy to see that

1. $\langle W, \leq, R \rangle$ forms an IM-frame, and
2. Let $\Vdash$ be the canonical valuation defined by: $T \Vdash p \iff p \in T$ for each propositional variable p. Then, $T \Vdash A \iff A \in T$ holds for each formula A.

Therefore, we only need to check that the canonical frame is indeed an IM$^{\bigcirc}$-frame. Below we check that it satisfies the condition of Definition 12 (2).

Lemma 16. *Let $S, T \in W$. Then, $\forall X \in W(T\ R\ X \iff S \subseteq X)$ if and only if $\bigcirc^{-1}T = S$.*

Proof. The right-to-left direction is obvious. To prove the other direction by contraposition, assume $\bigcirc^{-1}T \neq S$. Then we have either $\bigcirc^{-1}T \nsubseteq S$ or $S \nsubseteq \bigcirc^{-1}T$. In the first case, $T\ R\ X \iff S \subseteq X$ does not hold when $X = S$. In the second case, there exists some formula A such that $A \in S$ and $A \notin \bigcirc^{-1}T$. Then, in the usual way we can prove that there exists a prime theory V such that $\bigcirc^{-1}T \subseteq V$ and $A \notin V$ (therefore $T\ R\ V$ but $S \nsubseteq V$).

Lemma 17. *For $S, T \in W$ such that $S\ R\ T$, there exists a theory U (not necessarily prime) satisfying $\bigcirc^{-1}U = S$ and $T \subseteq U$.*

Proof. Let U be the set of all formulas provable from T and $\bigcirc S$. First, we check that U is a theory. It is clear that U is deductively closed. To check U is consistent, suppose $\bot \in U$. Then we have $\bigcirc\bot \in U$, hence $\bot \in \bigcirc^{-1}U = S$, a contradiction.

We are going to prove that $\bigcirc^{-1}U = S$ and $T \subseteq U$ hold for this U. Clearly, $T \subseteq U$ holds by definition. It is also easy to see that $S \subseteq \bigcirc^{-1}U$: if $A \in S$, then $\bigcirc A \in \bigcirc S \subseteq U$, and from this $A \in \bigcirc^{-1}U$ follows. For the converse, let A be a formula in $\bigcirc^{-1}U$. Then we have $\bigcirc A \in U$. Since U is the smallest theory containing T and $\bigcirc S$, there exist formulas $A_1, \ldots, A_n \in S$ $(n \geq 0)$ such that $\bigcirc A_1 \supset \ldots \supset \bigcirc A_n \supset \bigcirc A \in T$. Then, from axiom **CK**, we also have $\bigcirc(A_1 \supset \ldots \supset A_n \supset A) \in T$. This implies that $A_1 \supset \ldots \supset A_n \supset A \in \bigcirc^{-1}T \subseteq S$ holds. As $A_i \in S$ from the assumption, we conclude that $A \in S$, as required.

Lemma 18. *Let $S, T \in W$ such that $S\ R\ T$. Then, any maximal element of*

$$X = \left\{ U \;\middle|\; U \textit{ is a theory such that } \bigcirc^{-1}U = S \textit{ and } T \subseteq U \right\}.$$

is prime.

Proof. Let $U \in X$ be a maximal element and suppose $A_1, A_2 \notin U$. Moreover, let U_0, U_1, U_2 be the smallest theory extending U with $A_1 \vee A_2, A_1, A_2$, respectively. It is sufficient to prove that $U_0 \neq U$.

For $i = 1, 2$ the theory $\bigcirc^{-1}U_i$ is a proper extension of $\bigcirc^{-1}U = S$, so there exists a formula $B_i \in \bigcirc^{-1}U_i \setminus S$. For such B_1 and B_2, it holds that $\bigcirc(B_1 \vee B_2) \in U_1 \cap U_2 = U_0$ and $B_1 \vee B_2 \notin S = \bigcirc^{-1}U$ (because S is prime). Therefore we obtain $\bigcirc(B_1 \vee B_2) \in U_0 \setminus U$, and this implies $U_0 \neq U$, as required.

Putting these lemmas together, we can see that the canonical frame defined above is indeed an IM$^{\bigcirc}$-frame, from which the completeness follows.

The notion of IM-frames is first considered by Wolter and Zakharyaschev [12] (actually, in their terminology, IM-frames in this paper are called *Kripke* IM-frames) as a semantics for intuitionistic modal logic with $\Box$ as the only primitive modality. It is easy to see that most of the other variants of birelational Kripke frames can be reduced to IM-frames without changing satisfaction relation, as long as we consider only $\Box$ as a primitive modality. For example, functional frame semantics considered in subsection 5.1 can be translated into IM$^{\bigcirc}$-frame as follows:

Proposition 19. *For an arbitrary functional frame $\mathcal{F} = \langle W, \leq, R \rangle$, consider the binary relation $R' = (R\,; \leq)$. Then the frame $\mathcal{F}' = \langle W, \leq, R' \rangle$ is an* IM$^{\bigcirc}$*-frame, and for each satisfaction relation $\Vdash$ on W its extensions on $\mathcal{F}$ and $\mathcal{F}'$ coincide.*

5.3. Partially Functional Kripke Frames

We have established the soundness and completeness theorem, and therefore IM$^{\bigcirc}$-frames defined above capture our logic. However, while the logic is considered a version of LTL, the condition appearing in the definition of IM$^{\bigcirc}$-frames do not seem to justify linearity of time. Additionally, the intuitive meaning of the condition is not clear.

In this subsection we try to modify the semantics defined above so that the resulting semantics represents linear-time nature more directly. We consider another class of birelational Kripke frames, in which each state has at most one next state (although it may have no next state).

Definition 20. For an IM-frame $\langle W, \leq, R \rangle$, we define another relation R^s by

$$x \; R^s \; y \iff \forall z. (x \; R \; z \iff y \leq z).$$

Then, the condition appearing in the definition of IM$^{\bigcirc}$-frames (Definition 12 (2)) is rephrased by the equality $R = (\leq\, ; R^s)$. It is easy to check that the following properties also hold:

Lemma 21. *If $\langle W, \leq, R \rangle$ is an* IM$^{\bigcirc}$*-frame, then*

1. *R^s is a partial function;*
2. *R^s preserves $\leq$, that is, if $x \; R^s \; y$, $x' \; R^s \; y'$, and $x \leq x'$, then $y \leq y'$;*
3. *$(R^s)^{-1}$ is a simulation relation over $\langle W, \leq \rangle$. In other words, the inclusion $(R^s; \leq) \subseteq (\leq\, ; R^s)$ holds.*

This observation motivates the following definition.

Definition 22. Consider a triple $\langle W, \leq, S \rangle$ of a nonempty set W, a partial order $\leq$ on W and a partial function S on W. We say such a triple is an *intuitionistic partially functional frame* (IPF-frame, for short) if S preserves $\leq$. An IPF-frame is said to be an IPF$^{\bigcirc}$*-frame* if S^{-1} is a simulation relation over $\langle W, \leq \rangle$.

From Lemma 21, for each IM$^{\bigcirc}$-frame $\langle W, \leq, R\rangle$ we can construct an IPF$^{\bigcirc}$-frame $\langle W, \leq, R^s\rangle$ associated to it. We denote this construction by s. Conversely, each IPF$^{\bigcirc}$-frame gives rise to an IM$^{\bigcirc}$-frame $\langle W, \leq, (\leq ; S)\rangle$. It is easy to check that this is indeed an IM$^{\bigcirc}$-frame. We denote the construction of this direction by r. We also use the notation S^r for $(\leq ; S)$.

Moreover, we can show that r is a left-inverse of s. That is, when we construct an IPF$^{\bigcirc}$-frame from an arbitrary IM$^{\bigcirc}$-frame, and transforming it back to an IM$^{\bigcirc}$-frame, then the resulting frame is the same as the original one. This is an easy consequence of the equality $R = (\leq ; R^s)$ mentioned above.

The semantics based on IPF$^{\bigcirc}$-frames can be defined in the same way as before, except that we need to modify $\bigcirc$-clause as follows (otherwise, the heredity condition fails):

$$w \Vdash \bigcirc A \iff \forall w', v.(w \leq w' \; S \; v \implies v \Vdash A).$$

Because $w \leq w' \; S \; v$ in the right-hand side is equivalent to $w \; S^r \; v$, we have

$$w \Vdash \bigcirc A \iff \forall v.(w \; S^r \; v \implies v \Vdash A),$$

which is the same as the interpretation in IM-frame obtained by translation r.

Similarly, interpretation in an IM-frame is, since $R = (\leq ; R^s)$,

$$\begin{aligned} w \Vdash \bigcirc A &\iff \forall v.(w \; R \; v \implies v \Vdash A) \\ &\iff \forall w', v.(w \leq w' \; R^s \; v \implies v \Vdash A), \end{aligned}$$

so this is the same as the semantics on the IPF-frame obtained by s.

In this way we can see that two semantics based on IM$^{\bigcirc}$-frames and IPF$^{\bigcirc}$-frames are equivalent. Therefore IPF$^{\bigcirc}$-frames are another characterization of our logic.

5.4. Informal Interpretation of the Frame Conditions

Above we have proved that our logic is captured by either IM$^{\bigcirc}$-frames or IPF$^{\bigcirc}$-frames, but we did not discuss what their frame conditions mean. In this subsection we discuss the intuitive meaning of IPF$^{\bigcirc}$-frames.

The condition of IPF$^{\bigcirc}$-frames says that S^{-1} should be a simulation. According to the standard interpretation of Kripke semantics for intuitionistic logic, each possible world represents a state of knowledge, and $\leq$ represents an extension of knowledge. Following this interpretation, we can say that the condition that S^{-1} is a simulation relation says that any extension of knowledge at the next state can be simulated by some extension of knowledge at the current state. Actually this is achieved in such a way that the extension by gaining a knowledge A at the next state is simulated by the gaining $\bigcirc A$ at the current state (in fact, we implicitly used this intuitive understanding in the proof of completeness). Therefore, the simulation condition implies that we can indeed identify A^n and $\bigcirc^n A$.

In NJ$^{\bigcirc}$ formalization, the identification between A^n and $\bigcirc^n A$ is justified by rules $\bigcirc$I and $\bigcirc$E. From a type-theoretic viewpoint, this corresponds to the fact that $\lambda^{\bigcirc}$ can manipulate open code fragment, because if there is a side condition like other systems, quoted code fragments with free variables would not be well-typed.

In this way, we can see that (although informally) there is a connection between the Kripke semantics we gave and the characteristic feature of the typed λ-calculus $\lambda^{\bigcirc}$.

6. Concluding Remarks

6.1. Summary

In this paper we have investigated a constructive LTL. We first gave a natural deduction style proof system, and a sequent calculus which enjoys a cut elimination theorem. We also gave a Hilbert-style proof system. After that we defined Kripke semantics, and proved soundness and completeness.

Although the temporal logic we considered is *linear-time*, a naive frame condition of functionality turned out to be insufficient. We considered two classes of Kripke frames, and gave the connection between two versions of our semantics. We have also discussed relationship between frame conditions and syntactic counterpart of the logic.

For a cut elimination procedure, we basically followed the standard method. However, to make it work correctly, we may need extra transformations.

6.2. Two Kinds of Interpretation of Modality

Here we would like to discuss why the straightforward formalizations result in logics which do not meet our requirement. We rejected the distributivity law, and it is the natural consequence of a particular type-theoretic interpretation of $\bigcirc$ operator. However, we had to make some efforts to formalize such an LTL; we had to consider some extra side conditions in proof rules (like $\vee$E), and relatively complicated frame conditions in Kripke semantics.

We consider the origin of this difficulty is the difference between traditional way of interpreting modality and type-theoretic interpretation. Kripke semantics, which is a foundation of ordinary modal logics, is based on the idea that all possible worlds are equally observable. However, type theory (at least some of them, including $\lambda^{\bigcirc}$) do not seem to treat all worlds equally.

When we consider Kripke semantics, we implicitly assume that we are observing the whole system (Kripke frame), and accordingly we can inspect any state freely when judging whether a given formula is true or not. So we can say that the usual Kripke semantics assumes a viewpoint from *outside* of the system.

Type-theoretic point of view does not seem to assume such an ideal observer. Instead, it can be understood well if we consider observers *inside* the system. That is, an observer is assigned to each state, and a formula is considered true at some state only if the observer in the specified state is able to see that the formula is indeed true.

These two approaches result in different modal logics, and this explains why Kripke semantics tends to admit distributivity law (unless some special care is made), while it is plausible to reject the law in view of modal type systems. From the *outside*-view, the observer can freely go back and forth between states, and inspect future states to decide whether such and such property holds at the current state. If we take this point of view we can justify the distributivity law (in a constructive way):

> If we know that $A \vee B$ holds at the next state, then move to the next state and see which of A and B is actually the case. If A is the case we have $\bigcirc A$, and similarly for B. In either case we have $\bigcirc A \vee \bigcirc B$.

From the *inside*-view, however, each observer is assigned to a fixed state, and they cannot move to other states. As a result, the justification above do not correct. In such a setting it is possible to know that "either A or B holds at the next state" without knowing neither "A at the next state" nor "B at the next state."

As a result, to establish a Kripke semantics for type-theoretically motivated modal logic, it is necessary to emulate internal observers' states of knowledge in terms of possible worlds and accessibility relations. We consider this is the primary reason of the difficulty we have encountered in this paper.

6.3. Algebraic Semantics

In this paper we did not mention algebraic semantics and (topological and discrete) duality between frames and algebras [15]. Related to these topics, Wolter and Zakharyaschev [12] gave a general result on an intuitionistic analogue of topological duality. Also, a kind of discrete duality for constructive S4 and propositional lax logic are given by Alechina et al. [13].

It is not difficult to give a similar result for our constructive LTL. Consider a Heyting algebra equipped with a unary operation $\bigcirc$ preserving $\supset$, and call such an algebra a $\bigcirc$-algebra. It is easy to see that the class of $\bigcirc$-algebras gives a semantics of our constructive LTL together with soundness and completeness. In a way similar to the classical case, we can establish discrete duality between $\mathrm{IM}^{\bigcirc}$-frames and $\bigcirc$-algebras.

6.4. Related Work

The natural deduction system introduced in Section 2 is similar to those for intuitionistic modal logics by Martini and Masini [16] and by Simpson [10] (aside from a few notational differences), which also use formulas with annotations indicating where the formulas hold. However, there are some differences between their systems and ours. First, while our $\bigcirc$I rule does not have any side condition, $\Box$-introduction rules by Martini and Masini requires that all time annotations in the antecedent must be smaller than $n + 1$ (the time annotation of the succedent of the premise). There is also a similar condition in Simpson's one. Our $\bigcirc$I is actually more similar to $\Diamond$-introduction rule of Simpson's system. Second, $\vee$E and $\bot$E in our system are also different from theirs; these rules require time annotations of the succedents to be the same as the main formula, but it is not the case for the two. The absence of such a restriction allows us to prove distributivity of $\Diamond$ over disjunction in their systems.

Related to the issue discussed in Subsection 6.2, $\Diamond$ operator without distributivity or $\Diamond\bot \supset \bot$ has been discussed in the literature [9, 11, 17, 13]. In particular, Kripke semantics for propositional lax logic by Fairtlough and Mendler [11] and constructive S4 by Alechina et al. [13] had to consider *fallible worlds*, possible worlds at which any proposition becomes true.

Also, Murphy et al. [18] consider a typed λ-calculus for distributed computation, which corresponds to intuitionistic S5 modal logic. Their system is based on natural deduction formalization by Simpson [10]. Although the system they formalized is an implicational fragment, they discuss how to add other connectives, and point out that $\bot$ and $\vee$ need special consideration. In particular, when $\vee$ is added, it is not obvious how to define operational semantics for case splitting. This is because, as they mention, the elimination rule for $\vee$ and $\bot$ in Simpson's system reasons *non-locally*, that is, main premise and conclusion may have different annotations. There is a similarity between this difficulty and the issue we have discussed in Subsection 6.2.

Since work by Davies and Pfenning [19] and Davies [3] on Curry-Howard correspondence for modal and temporal logic, many type systems for multi-stage languages based on their work have been proposed [20, 21, 22, 23, 24, 25, 8, 26, 27]. Those languages typically include not only quasiquotation as in $\lambda^{\bigcirc}$ but also Lisp-like eval and lifting of values to code (also called cross-stage persistence [23]). As a result, their type systems could be seen as quite different modal logics: for example, the distributivity law would be validated if eval, which would have type $\bigcirc A \supset A$, and lifting, which would have type $A \supset \bigcirc A$, are supported in one language. The combination of these language features is motivated by a practical reason, rather than a correspondence with logics; it would also be interesting to investigate how these systems (more precisely, the corresponding logics) are characterized in terms of temporal or modal logics. The second author makes such investigations [8, 27], which tries to capture quasiquotation and eval by modalities like next and always in temporal logic.

References

[1] P. Maier, Intuitionistic LTL and a new characterization of safety and liveness, in: Proceedings of Conference of the European Association for Computer Science Logic, Vol. 3210 of Lecture Notes in Computer Science, Springer Verlag, 2004, pp. 295–309.

[2] W. B. Ewald, Intuitionistic tense and modal logic, Journal of Symbolic Logic 51 (1) (1986) 166–179.

[3] R. Davies, A temporal-logic approach to binding-time analysis, in: Proceedings of IEEE Symposium on Logic In Computer Science (LICS'96), 1996, pp. 184–195.

[4] N. D. Jones, C. K. Gomard, P. Sestoft, Partial Evaluation and Automatic Program Generation, Prentice-Hall, 1993.

[5] R. Glück, J. Jørgensen, Efficient multi-level generating extensions for program specialization, in: Proceedings of Programming Languages, Implementations, Logics and Programs (PLILP'95), Vol. 982 of Lecture Notes in Computer Science, 1995, pp. 259–278.

[6] K. Kojima, A. Igarashi, On constructive linear-time temporal logic, in: Proceedings of the Intutionistic Modal Logics and Applications Workshop (IMLA'08), 2008.

[7] C. Stirling, Modal and temporal logics, in: Handbook of Logic in Computer Science, Oxford University Press, Inc., New York, NY, USA, 1992, pp. 477–563.

[8] Y. Yuse, A. Igarashi, A modal type system for multi-level generating extensions with persistent code, in: Proceedings of 8th ACM SIGPLAN Symposium on Principles and Practice of Declarative Programming (PPDP'06), Venice, Italy, 2006, pp. 201–212.

[9] D. Wijesekera, Constructive modal logics I, Annals of Pure and Applied Logic 50 (1990) 271–301.

[10] A. K. Simpson, The proof theory and semantics of intuitionistic modal logic, Ph.D. thesis, University of Edinburgh (1994).

[11] M. Fairtlough, M. Mendler, Propositional lax logic, Information and Computation 137 (1) (1997) 1–33.

[12] F. Wolter, M. Zakharyaschev, Intuitionistic modal logics as fragments of classical bimodal logics, Logics at work, Essays in honour of Helena Rasiowa (1999) 168–186.

[13] N. Alechina, M. Mendler, V. de Paiva, E. Ritter, Categorical and Kripke semantics for constructive S4 modal logic, in: L. Fribourg (Ed.), Proceedings 15th Int. Workshop on Computer Science Logic, CSL'01, Paris, France, 10–13 Sept. 2001, Vol. 2142, Springer-Verlag, Berlin, 2001, pp. 292–307.

[14] K. Segerberg, Modal logics with functional alternative relations., Notre Dame Journal of Formal Logic 27 (4) (1986) 504–522.

[15] Y. Venema, Algebras and co-algebras, in: P. Blackburn, J. van Benthem, F. Wolter (Eds.), Handbook of Modal Logic, Vol. 3 of Studies in Logic and Practical Reasoning, Elsevier Science, 2006, Ch. 6, pp. 331–426.

[16] S. Martini, A. Masini, A computational interpretation of modal proofs, in: H. Wansing (Ed.), Proof Theory of Modal Logics, Kluwer, 1994, pp. 213–241.

[17] S. Kobayashi, Monad as modality, Theoretical Computer Science 175 (1997) 29–74.

[18] T. Murphy, VII, K. Crary, R. Harper, F. Pfenning, A symmetric modal lambda calculus for distributed computing, in: Proceedings of the 19th Annual IEEE Symposium on Logic In Computer Science (LICS 2004), 2004, pp. 286–295.

[19] R. Davies, F. Pfenning, A modal analysis of staged computation, J. ACM 48 (3) (2001) 555–604.

[20] Z. E.-A. Benaissa, E. Moggi, W. Taha, T. Sheard, Logical modalities and multi-stage programming, in: Proceedings of Workshop on Intuitionstic Modal Logics and Applications (IMLA'99), 1999.

[21] E. Moggi, W. Taha, Z. E.-A. Benaissa, T. Sheard, An idealized MetaML: Simpler, and more expressive, in: Proceedings of European Symposium on Programming (ESOP'99), Vol. 1576 of Lecture Notes in Computer Science, 1999, pp. 193–207.

[22] W. Taha, M. F. Nielsen, Environment classifiers, in: Proceedings of ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'03), 2003, pp. 26–37.

[23] W. Taha, T. Sheard, MetaML and multi-stage programming with explicit annotations, Theoretical Computer Science 248 (2000) 211–242.

[24] E. Moggi, S. Fagorzi, A monadic multi-stage metalanguage, in: Proceedings of Conference on Foundations of Software Science and Computation Structures (FoSSaCS'03), Vol. 2620 of Lecture Notes in Computer Science, Springer Verlag, 2003, pp. 358–374.

[25] A. Nanevski, F. Pfenning, Staged computation with names and necessity, Journal of Functional Programming 15 (5) (2005) 893–939.

[26] I.-S. Kim, K. Yi, C. Calcagno, A polymorphic modal type system for Lisp-like multi-staged languages, in: Proceedings of ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'06), Charleston, SC, 2006, pp. 257–268.

[27] T. Tsukada, A. Igarashi, A logical foundation for environment classifiers, in: P.-L. Curien (Ed.), Proceedings of the 9th International Conference on Typed Lambda-Calculi and Applications (TLCA'09), Vol. 5608 of Lecture Notes in Computer Science, Springer Verlag, 2009, pp. 341–355.