On Constructive Linear-Time Temporal Logic

Kensuke Kojima[1] and Atsushi Igarashi[2]

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 and Kripke semantics for constructive LTL with conjunction and disjunction, and prove soundness and completeness. Distributivity of the "next" operator over disjunction "$\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$" is rejected from a computational viewpoint. We also give a formalization by sequent calculus and its cut-elimination procedure.

Keywords: 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 may depend 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 system, is temporal logic in which each time has a unique time that follows it.

Davies [3] 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 [8] to determine which part of a program can be computed at specialization-time and which is residualized. He defined a natural deduction system for a constructive LTL with only the "next" operator $\bigcirc$ and implication, 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 [6]. 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

[1] Email: kozima@kuis.kyoto-u.ac.jp
[2] Email: igarashi@kuis.kyoto-u.ac.jp

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 $\texttt{parser\_spec} \to \bigcirc(\texttt{string} \to \texttt{syntax\_tree})$. Unfortunately, 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.

In this paper we study logical aspects of constructive propositional LTL based on Davies' formalization. Davies' original system is an implicational fragment, but we also consider conjunction and disjunction.[3] Our contributions are (1) to give a Kripke semantics and a complete proof system for constructive LTL and (2) to give another formalization by sequent calculus in which cut elimination holds.

Intuitionistic versions of LTL have been already considered in the literature [9,4]. However, the LTL presented in this paper is motivated by the type-theoretic interpretation of $\bigcirc A$ as a type of quoted code, which distinguishes our approach from others. In fact, our version of LTL is not equivalent to the intuitionistic LTLs previously considered in 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. The reason we disallow this law will be discussed later.

The organization of the rest of this paper is as follows. In Section 2, we discuss an implicational fragment: we first review the natural deduction by Davies, give a Kripke semantics, obtained by a natural extension of that of the classical LTL, and finally prove soundness and completeness of the proof system. We also discuss that, unfortunately, a straightforward extension of the semantics to disjunction is not suitable for our interpretation of disjunction. In Section 3 we extend the logic with conjunction and disjunction. We give another Kripke semantics, which does not admit the distributivity law mentioned above, and prove soundness and completeness of the proof system. In Section 4 we define a sequent calculus $\mathrm{LJ}^{\bigcirc}$, which is equivalent to the natural deduction, with its cut elimination procedure. Finally, we give concluding remarks in Section 5.

2 Implicational Fragment

In this section, we first recall the natural deduction system by Davies and some of its properties, define a Kripke semantics for it, and prove completeness of Davies' system.

2.1 Results by Davies

The temporal logic Davies considered contains only $\bigcirc$ ("next" operator) and $\supset$ (intuitionistic implication), so the language we consider in this section is constructed from propositional variables using $\supset$ and $\bigcirc$.

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

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

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

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

Fig. 1. Derivation Rules of Davies' System.

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 Fig. 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 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 [12]. 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 2.1 *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 Kripke Semantics via Functional Frames

Before discussing the semantics of the implicational fragment, we briefly explain how the usual classical semantics is given in terms of Kripke semantics. Kripke frames we consider are *functional*, in the sense that the accessibility relation R on possible worlds is a map.[4] This condition guarantees that, in a functional frame, the next state of a given state is uniquely determined, hence justifying "linear time".

To give a semantics of constructive LTL, we follow the previous researches on Kripke-style models of intuitionistic modal logics [1,14,2] and augment functional frames by another accessibility relation $\leq$. This additional accessibility represents the "constructive" counterpart, as in the standard semantics of intuitionistic logic.

Definition 2.2 *An* intuitionistic functional frame *is a triple $\langle W, \leq, R\rangle$ of a nonempty set W, a preorder $\leq$ on W and a map R from W to W such that $\leq \circ R = R \circ \leq$ holds. Here $\circ$ stands for a composition of binary relations defined by $x\ R \circ S\ y \iff \exists z.(x\ R\ z\ S\ y)$.*

This notion is an extension of classical functional frames: if $\leq$ is the diagonal relation (that is, $x \leq y$ if and only if $x = y$) in this definition, the frame $\langle W, \leq, R\rangle$ can be identified with a classical functional frame $\langle W, R\rangle$. Hereafter, we simply say functional frame when no confusion arises.

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

Definition 2.3 *Let $\langle W, \leq, R\rangle$ be a functional frame and $\models$ be a binary relation between W and the set of propositional variables such that $w \leq w'$ and $w \models p$ imply $w' \models p$. We extend $\models$ to formulas by induction with*

- *$w \models A \supset B \iff$ if $w \leq w'$ and $w' \models A$ then $w' \models B$, and*
- *$w \models \bigcirc A \iff$ if $w\ R\ w'$ then $w' \models A$.*

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

This definition is one of the standard semantics of intuitionistic modal logics previously considered [14]. As is easily verified by induction on the construction of formulas, this semantics satisfies the monotonicity condition.

Lemma 2.4 *If $w \leq w'$ and $w \models A$, then $w' \models A$.*

It is not very difficult to see that the Davies' system is sound and complete for this semantics. Soundness is proved by straightforward induction on the derivation. Completeness is proved by constructing a functional frame in which validity and provability coincide. We sketch the proof 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 as W, let $\leq$ be a set-inclusion, and R the map which sends each theory T to the theory $\bigcirc^{-1}T$. First we show that this defines a functional frame.

Lemma 2.5 *The canonical frame $\langle W, \leq, R\rangle$ above is indeed functional.*

Proof. Among conditions of being a functional frame, the only nontrivial one is $R \circ \leq\ \subseteq\ \leq \circ R$. To show this, take theories T and S with $\bigcirc^{-1}T \subseteq S$ (i.e. $T\ (R \circ \leq)\ S$), and let U be the smallest theory containing T and $\bigcirc S$. We are going to show that U satisfies $T \leq U\ R\ S$, i.e. $T \subseteq U$ and $\bigcirc^{-1}U = S$.

Clearly, $T \subseteq U$ holds by definition. It is also easy to see that $S \subseteq \bigcirc^{-1}U$: if

[4] The term "functional" is, to our knowledge, first used by Segerberg [11], but not in context of semantics of LTL.

$A \in S$, 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 $A_1, \ldots, A_n \in S$ such that $\bigcirc A_1 \supset \ldots \supset \bigcirc A_n \supset \bigcirc A \in T$. Because $\bigcirc(A \supset B)$ follows from $\bigcirc A \supset \bigcirc B$, 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. □

Let $\models$ be the satisfaction relation defined by: $T \models p$ if and only if $p \in T$. Then it holds that $T \models A$ if and only if $A \in T$ for each formula A, which is easily verified by induction on A. Finally, if $\Gamma \vdash A^n$ is not provable, take the set $\left\{ A \,\middle|\, \Gamma \vdash A^0 \right\}$ as T. Then $T \models \Gamma$ holds but $T \models A^n$ does not.

2.3 A Problem with Disjunction

The proof strategy above is almost standard, but notice that we took the set of all theories as W. When we consider the full system (in particular, disjunction), the same method will not work. In the presence of disjunction, the standard way to prove completeness is to take the set of all *prime*.[5] Otherwise, we cannot prove the equivalence of $T \models A$ and $A \in T$ in the last step of the proof above. However, if we give W in this way, there is no natural way to define suitable R because the theory $\bigcirc^{-1} T$ is not necessarily prime even if T is prime.

In fact, functional frames are not appropriate in the presence of disjunction because they would validate the *distributivity law* $\bigcirc(A \vee B) \supset \bigcirc A \vee \bigcirc B$ under the straightforward interpretation of disjunction:

$$w \models A \vee B \iff \text{if } w \models A \text{ or } w \models B$$

According to our type-theoretic interpretation of $\bigcirc$, this formula should not be valid. By the Curry-Howard correspondence, a proof of the distributive 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*; it is in general impossible to know which value (A or B) this code evaluates to *now*. 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 $\bigcirc(A \vee B)$.

It does not seem easy to adjust the definition of the satisfaction relation to exclude the distributivity law. In fact, since necessity and possibility coincide when R is a (total) map, it may appear natural to adopt the ideas from some of the Kripke semantics for intuitionistic modal logics [13,1], which rejects distributivity $\Diamond(A \vee B) \supset \Diamond A \vee \Diamond B$ of possibility over disjunction by:

$$w \models \Diamond A \iff \forall v.(w \leq v \implies \exists w'.(v \mathrel{R} w' \wedge w' \models A)).$$

Unfortunately, this attempt fails. To falsify the distributivity we also need to have $\leq \circ R \not\subseteq R \circ \leq$, but then, the formula $(\bigcirc A \supset \bigcirc B) \supset \bigcirc(A \supset B)$ becomes not

[5] A theory T is said to be prime if $A \vee B \in T$ implies $A \in T$ or $B \in T$.

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

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

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

Fig. 2. Additional Rules for Full $\text{NJ}^{\bigcirc}$

valid. Indeed, consider a functional frame $\langle W, \leq, R\rangle$ defined by $W = \{a, b, c, d\}$ and $\leq\ = \{(a, b), (a, a), (b, b), (c, c), (d, d)\}$ and $R = \{(a, c), (b, d), (c, c), (d, d)\}$ and the satisfaction relation such that A is true at c and false at d, and B is false at c. Then, $a \models \bigcirc A \supset \bigcirc B$ holds but $a \models \bigcirc(A \supset B)$ does not.

From the observation above, it seems that functionality of R and soundness implies the distributivity. In the next section we give a larger class of frames, by relaxing the functionality condition.

3 Full System: Natural Deduction and Kripke Semantics

In the previous section we have seen that the notion of functional frames is too naive to represent the intuitive meaning of the $\bigcirc$ operator we consider. In this section we propose a more suitable class of Kripke frames and a complete proof system.

3.1 Natural Deduction

First we define a natural deduction system $\text{NJ}^{\bigcirc}$ extending Davies' system, by adding conjunction and disjunction. Derivation rules for these two connectives are listed in Fig. 2. They are fairly straightforward, but only $\vee$E may be nontrivial. In this rule, 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:

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

In this proof, disjunction being eliminated has time 1 while the time of the succedent is 0. In fact, the problem would occur only if we allowed the time of the succedent C to be strictly less than that of the disjunction $A \vee B$ 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.)

3.2 *Kripke Semantics*

As discussed above, the proof system NJ$^{\bigcirc}$ does not seem to prove distributivity law, so we think the logic defined by NJ$^{\bigcirc}$ is more appropriate than that by functional frames. Therefore the next question is what kind of frames correspond to our logic. The answer we give is $\bigcirc$-frames, defined below.

Definition 3.1 *A $\bigcirc$-frame is a triple $\langle W, \leq, R\rangle$ of a nonempty set W, a preorder $\leq$ on W and a binary relation R on W such that*

- $\leq \circ R = R \circ \leq = R$, *and*
- *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, here, R is not assumed to be a map. This definition is essentially a special case of Kripke IM-frames considered by Wolter and Zakharyaschev [14].

Satisfaction relations are defined in the same way as the functional frame semantics in Section 2, but we need to add the following two clauses for disjunction and conjunction.

- $w \models A \vee B \iff w \models A$ or $w \models B$
- $w \models A \wedge B \iff w \models A$ and $w \models B$

This $\bigcirc$-frame semantics is a generalization of the functional one:

Proposition 3.2 *For an arbitrary functional frame $\mathcal{F} = \langle W, \leq, R\rangle$, there exists a binary relation R' such that the frame $\mathcal{F}' = \langle W, \leq, R'\rangle$ is a $\bigcirc$-frame, and for each satisfaction relation $\models$ on W its extensions on $\mathcal{F}$ and $\mathcal{F}'$ coincide.*

Proof. Let $R' = R \circ \leq$ (in other words, $w\ R'\ v$ if and only if $u \leq v$, where u is the image of R at w). Then $\leq \circ R' = R' \circ \leq = R'$ is easily verified from $\leq \circ R = R \circ \leq$ and transitivity of $\leq$. The latter part is proved by induction on the formula. □

Theorem 3.3 (Soundness) *Suppose that $\Gamma \vdash A^n$ is provable in NJ$^{\bigcirc}$. Then for any $\bigcirc$-frame $\langle W, \leq, R\rangle$, satisfaction relation $\models$, and possible world $w \in W$ such that $w \models \Gamma$, it holds that $w \models A^n$.*

Proof. Induction on the derivation. □

Theorem 3.4 (Completeness) *If $w \models \Gamma$ implies $w \models A^n$ for any $\bigcirc$-frame $\langle W, \leq, R\rangle$, satisfaction relation $\models$, and possible world $w \in W$, then there exists a derivation of $\Gamma \vdash A^n$.*

Proof. Basically we proceed in a way similar to the proof in Section 2, but we need some modification. Here we we take the set of all *prime* theories as W, and define accessibility relation R so that $T\ R\ T'$ holds if and only if $\bigcirc^{-1}T \subseteq T'$.

The only nontrivial point in the proof is that $\langle W, \leq, R\rangle$ defined above is indeed a $\bigcirc$-frame. The condition $\leq \circ R = R \circ \leq = R$ is not difficult to prove, and we omit the details. Below we prove that the other condition is satisfied. Let S and T be prime theories such that $T\ R\ S$ (i.e. $\bigcirc^{-1}T \subseteq S$). Our goal is to prove that there exists some prime theory U such that $T \subseteq U$ and $\forall V \in W.(\bigcirc^{-1}U \subseteq V \iff S \subseteq V)$. Let X be the set of theories defined by:

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

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

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

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

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

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

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

Fig. 3. Inference Rules of $\mathrm{LJ}^{\bigcirc}$.

We are going to show that X is not empty, and its maximal element is a prime theory. For the former, take the smallest theory containing T and $\bigcirc S$ and show that it belongs to X. This is done in the same way as in the last section. To prove the latter, 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 containing $A_1 \vee A_2, A_1, A_2$, respectively, and U. 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.

The rest of the proof is almost the same as the previous one. □

4 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 $\mathrm{LJ}^{\bigcirc}$.

4.1 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 left-hand side of the initial sequents. To make the proof of cut elimination theorem simpler, we restricted the right-hand side of the initial sequents to be atomic (but this does not reduce the proof-theoretic strength). Most of the rest of the rules are standard, but we comment on the rule $\vee$L. In this rule, the time of the succedent C must be no less than that of the principal formula $A \vee B$. This corresponds to the issue mentioned in the previous section that we cannot eliminate disjunction with a succedent of an earlier time.

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

Theorem 4.1 *A sequent* $\Gamma \Rightarrow F$ *is provable in* $LJ^{\bigcirc}$ *if and only if* $\Gamma \vdash F$ *is provable in* $NJ^{\bigcirc}$*.*

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

Lemma 4.2 (i) *If* $\Gamma \vdash F$ *is provable, then* $\Gamma, \Delta \vdash F$ *is also provable.*

(ii) *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.

4.2 Cut Elimination Procedure

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

Theorem 4.3 *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 four cases:

(i) $R_1 \neq \vee\text{L}$ or $R_2 = \text{Init}$;

(ii) $R_1 = \vee\text{L}$ and F is not principal in $\mathcal{D}_2$;

(iii) $R_1 = R_2 = \vee\text{L}$ and F is principal in $\mathcal{D}_2$;

(iv) $R_1 = \vee\text{L}$, F is principal in $\mathcal{D}_2$, and F is neither atomic nor disjunction.

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

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

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

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

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, (ii), (iii), and (iv) listed above.

In case (ii) 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 $\mathcal{D}_2$.

In case (iii), we can use the standard procedure above because the condition $n \leq l$ is always met.

The last case is the case (iv), 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 a right rule application. 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 4.4 *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. See Appendix A. □

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

Theorem 4.5 *If a sequent is provable in $\mathrm{LJ}^{\bigcirc}$, then it has a cut-free proof.*

5 Concluding Remarks

In this paper we have defined a Kripke semantics for constructive LTL, a sound and complete natural deduction style proof system, and a sequent calculus which enjoys a cut elimination theorem.

Although the temporal logic we considered is *linear-time*, a naive frame condition of functionality turned out to be insufficient, and we used a larger class of Kripke frames. Compared to other modal logics such as S4 and lax logic, an intuitive meaning of the frame condition we presented is not so clear, but it seems to correspond to the fact that the inverse of axiom **K** is a theorem.

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

In this paper we did not mention algebraic semantics and duality between frames and algebras. Related to these topics, results for constructive S4 and propositional lax logic are given by Alechina et al. [1]. A similar result also holds for our constructive LTL. Let us call a lattice equipped with a unary operation $\bigcirc$ a $\bigcirc$-algebra if it has pseudo-complement $\supset$ and $\bigcirc$ preserves $\supset$. It is fairly easy to see that the $\bigcirc$-algebras derive a semantics of constructive LTL and that $\mathrm{NJ}^{\bigcirc}$ is sound and complete. In a way similar to the classical case we can define translations between $\bigcirc$-frames and $\bigcirc$-algebras. Further investigations are left for future work. On duality for intuitionistic modal logics, Wolter and Zakharyaschev [14] also gave a general result, but it does not directly give rise to duality between $\bigcirc$-frame and some class of algebras. This is because we used Kripke frames while they considered general frames.

In the context of multi-modal and intuitionistic modal logics, a notion of product of Kripke frames and general frames are considered [5,7]. We conjecture that there exists a decomposition of functional frame (and maybe $\bigcirc$-frame) into a product of frames.

Another interesting problem is to consider temporal operators other than $\bigcirc$, such as "always" or "until". It is easy to define a semantics for other temporal operators, so the main interest is how to characterize these operators in terms of proof systems. In relation with this issue, a completeness result for constructive propositional dynamic logic is given by Nishimura [10]. Dynamic logic has operators similar to temporal operators, including "next" operator, so we think there are some relationship between his work and ours.

References

[1] Natasha Alechina, Michael Mendler, Valeria de Paiva, and Eike Ritter. Categorical and Kripke semantics for constructive S4 modal logic. In L. Fribourg, editor, *Proceedings 15th Int. Workshop on Computer Science Logic, CSL'01, Paris, France, 10–13 Sept. 2001*, volume 2142, pages 292–307. Springer-Verlag, Berlin, 2001.

[2] Milan Božić and Kosta Došen. Models for normal intuitionistic modal logics. *Studia Logica*, 43(3):217–245, September 1984.

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

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

[5] Dov M. Gabbay and Valentin B. Shehtman. Products of modal logics, part 1. *Logic Journal of the IGPL*, 6(1):73–146, January 1998.

[6] Robert Glück and Jesper Jørgensen. Efficient multi-level generating extensions for program specialization. In *Proceedings of Programming Languages, Implementations, Logics and Programs (PLILP'95)*, volume 982 of *Lecture Notes in Computer Science*, pages 259–278, 1995.

[7] Yasusi Hasimoto. *Algebras and Frames for Modal Logics.* PhD thesis, School of Information Science, Japan Advanced Institute of Science and Technology, January 2001.

[8] Neil D. Jones, Carsten K. Gomard, and Peter Sestoft. *Partial Evaluation and Automatic Program Generation.* Prentice-Hall, 1993.

[9] Patrick Maier. Intuitionistic LTL and a new characterization of safety and liveness. In *Proceedings of Conference of the European Association for Computer Science Logic*, volume 3210 of *Lecture Notes in Computer Science*, pages 295–309. Springer Verlag, 2004.

[10] Hirokazu Nishimura. Semantical analysis of constructive PDL. *Publications of the Research Institute for Mathematical Sciences*, 18:847–858, 1982.

[11] Krister Segerberg. Modal logics with functional alternative relations. *Notre Dame Journal of Formal Logic*, 27(4):504–522, October 1986.

[12] Colin Stirling. Modal and temporal logics. In *Handbook of Logic in Computer Science*, pages 477–563. Oxford University Press, Inc., New York, NY, USA, 1992.

[13] Duminda Wijesekera. Constructive modal logics I. *Annals of Pure and Applied Logic*, 50:271–301, 1990.

[14] Frank Wolter and Michael Zakharyaschev. Intiuitionistic modal logics as fragments of classical bimodal logics. *Logics at work, Essays in honour of Helena Rasiowa*, pages 168–186, 1998.

A Proof of Lemma 4.4

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

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

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

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

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

Other cases are similar.