National Institute of
Advanced Industrial Science
and Technology
AIST

AIST-PS-2007-005

Simulations of Multi-Valued Models for Modal μ-Calculus

Koki Nishizawa Yukiyoshi Kameyama Yoshiki Kinoshita

CVS, AIST University of Tsukuba CVS, AIST

算譜科学研究速報
Programming Science
Technical Report

Research Center
for Verification and Semantics

独立行政法人 産業技術総合研究所 システム検証研究センター 発行
Published by Research Center for Verification and Semantics
National Institute of Advanced Industrial Science and Technology

Simulations of Multi-Valued Models for Modal μ-Calculus

Koki Nishizawa[1] Yukiyoshi Kameyama[2] Yoshiki Kinoshita[1] *

[1] Research Center for Verification and Semantics (CVS),
National Institute of Advanced Industrial Science and Technology (AIST)
1-2-14 Shin-Senri Nishi, Toyonaka, Osaka 560-0083, Japan
koki-nishizawa@aist.go.jp
yoshiki@m.aist.go.jp
[2] Department of Computer Science,
Graduate School of Systems and Information Engineering,
University of Tsukuba
1-1-1 Tennodai, Tsukuba, 305-8573, Japan
kameyama@acm.org

Abstract

We study multi-valued Kripke models of propositional modal μ-calculus and simulations between them. We argue that the set of truth values must form a frame (complete Heyting algebra) in order for the multi-valued relations and small sets to form a category. We then show the simulation theorem, which says that the truth values of universal formulae are preserved through a multi-valued simulation. We treat models of state formulae and path formulae in a uniform way through "the path model construction," which gives a path model from a given (state) model. A relation between state models is lifted to that between path models; surprisingly, however, some simulation between state models can never be lifted to a simulation. After giving such an example, we show our main theorem, which gives a sufficient condition on the truth value frame for any simulation to be lifted to a simulation by path model construction.

Keywords: Modal μ-Calculus, Multi-Valued Model Checking, Simulation Theorem, Complete Heyting Algebra, Category.

*This research was supported by Core Research for Evolutional Science and Technology (CREST) Program "New High-Performance Information Processing Technology Supporting Information-oriented Society" of Japan Science and Technology Agency (JST).

1 Introduction

Multi-valued model checking is studied extensively by Chechik, Gurfinkel and others [1, 8]. They give the notion of multi-valued Kripke model of temporal logics, and develop an efficient model checking algorithm with respect to such models. Their multi-valued Kripke structure takes truth values in a de Morgan algebra to represent notions related to partiality of information such as being "unknown," "uncertain" and "inconsistent." Multi-valued model checking also makes it possible to perform a number of two-valued model checking all at once, by superposing many two-valued models and checking the resulting multi-valued model.

We address the notion of simulation in the multi-valued context. To give their foundation, we seek for the definitive lattice structure of truth values as well as a good formulation of relations weighted over it. We are interested in giving interpretations for path formulae and state formulae in a uniform manner.

We first examine what should be the multi-valued relations, since they are fundamental in multi-valued model checking. Small sets and two-valued binary relations inbetween form an *allegory* [5], a category with added structure, and most relational properties are derived from this structure. So, it would be natural to expect that multi-valued relations also form one. Apparently, the truth values for such relations should have a partial order, but the partially ordered sets must form a *frame (complete Heyting algebra)* in order for those relations to form a category [11]. Therefore, we formulate the notion of multi-valued Kripke structure which takes truth values in a frame, and define multi-valued Kripke model of an intuitionistic variant of Kozen's modal μ-calculus [13].

The simulation theorem already appears in the book [3]. It states that, if a formula in a certain form is valid in a Kripke model, then it is also valid in all Kripke models simulated by the former. We show the simulation theorem also holds in our multi-valued setting.

Then we give a construction of a model from a given model. The former is called the "path model" and the latter is called the "state model" in this context. The states of the path model are infinite sequences of states of the state model, so path formulae can naturally be interpreted in the path model. The path model construction also lifts a multi-valued relation between state models to one between their path models. One hopes that the lifted relation is always a simulation relation, provided the original relation is a simulation, but we give a counterexample for that. Our main theorem gives a sufficient condition on the truth value frame for a lifted relation to be a simulation.

Our contributions are summarised as follows.

- We take *frames* to be the structure of truth values in our formulation of the multi-valued Kripke models for intuitionistic modal μ-calculus. This structure is definitive in the sense that frame is necessary and sufficient structure for the multi-valued relations to form a category under a certain definition of the composition.

- We introduce *multi-valued simulations* between multi-valued Kripke struc-

tures. These are necessary in order to superpose simulation relations. Thanks to our category theoretical formulation, we can not only define multi-valued simulations without any fuss, but also prove the simulation theorem more shortly than in an element-wise way.

- We give a systematic construction of the path model from a given (state) model, and examine how a simulation relation between the state models is lifted to a relation between the path models. We give an example of simulation relations which can be lifted to no simulation relations between path models. Our main theorem gives a sufficient condition on the truth value frame for an arbitrary simulation relation to be lifted to a simulation relation between path models.

This paper is organised as follows. Section 2 introduces relations weighted over a frame. In Section 3, we extend the notion of multi-valued Kripke structure and that of simulation between them. We then introduce the validity of intuitionistic modal μ-formulae in the multi-valued Kripke models and in the path models, in Sections 4 and 5, respectively. Finally, our main theorem is proved in Section 6. Section 7 compares our work with other works [4, 1, 8]. Section 8 summarises this work and future work.

2 Multi-Valued Relations in Category $\mathbf{Mat}(L)$

In this section, we formulate the notion of multi-valued relation. Our formulation is based on the following scenario. Given two sets X and Y, an ordinary binary relation from X to Y can be regarded as a function of $X \times Y \longrightarrow 2$ where 2 is the set consisting of the truth values "true" and "false". We may replace 2 by an arbitrary set L of truth values. Thus we call a function from $X \times Y$ to L an *L-valued relation from X to Y*.

We take a *frame* (i.e., a complete lattice whose binary meets distribute over arbitrary joins) to be the structure of truth values, since it is necessary and sufficient for the multi-valued relations to form a category as we will see later in this section. In this section, we review the category $\mathbf{Mat}(L)$, in which our work in this paper is formulated, following Johnstone [11].

We do not distinguish binary meets $\wedge$ and joins $\vee$ from infinitary ones, and use the same symbols for them. We write $\bot$ and $\top$ for the least and greatest elements, respectively. We write $[S, L]$ for the frame of all functions from a set S to a frame L with the pointwise order.

A complete lattice is a frame if and only if it is a Heyting algebra. So, we sometimes regard a frame as a *complete Heyting algebra*. For $x, y \in L$, the element $x \Rightarrow y \stackrel{\text{def}}{=} \bigvee\{z \in L \mid x \wedge z \leq y\}$ satisfies that $x \wedge w \leq y$ if and only if $w \leq x \Rightarrow y$ for all $w \in L$.

$\mathbf{Mat}(L)$ is a category whose objects are small sets and morphisms are binary relations weighted over L.

Definition 2.1 (Category $\mathbf{Mat}(L)$ [11])**.** Let L be a frame. The following data form a category $\mathbf{Mat}(L)$.

- $\mathrm{ob}(\mathbf{Mat}(L)) \stackrel{\mathrm{def}}{=}$ small sets.
- $\mathbf{Mat}(L)(X,Y) \stackrel{\mathrm{def}}{=} \{\, f\colon X \times Y \longrightarrow L \mid f \text{ is a function} \,\}$, for $X,\ Y \in \mathrm{ob}(\mathbf{Mat}(L))$.
- $\mathrm{id}_X(x,x') \stackrel{\mathrm{def}}{=} \begin{cases} \top & \text{if } x = x' \\ \bot & \text{otherwise.} \end{cases}$
- $(S \circ R)(x,z) \stackrel{\mathrm{def}}{=} \bigvee\{\, S(y,z) \wedge R(x,y) \mid y \in Y \,\}$, for $R \in \mathbf{Mat}(L)(X,Y)$ and $S \in \mathbf{Mat}(L)(Y,Z)$.

The arrow of $\mathbf{Mat}(L)$ is called an *L-valued relation*.

We write $R\colon X \nrightarrow Y$ for $R \in \mathbf{Mat}(L)(X,Y)$ when L is clearly determined from the context. At a first glance one might naïvely conclude it is sufficient for L to be a partially ordered set, but for the well-formedness of the composition, L has to be a complete lattice. Moreover, for the associativity of the composition to hold, L has to be a frame.

The idea of weighted relations is classical. L-valued relation can be seen, for instance, as a special case of L-relation introduced by Goguen [7] where the frame is equipped with a monoid structure. On the other hand, fuzzy relations (see, e.g., [6]) are special cases of L-valued relations where L is the frame of the closed interval $[0,1]$. We do not see, however, any reason for introducing extra monoid structure upon frame, nor for restricting L to a closed interval, for our purpose.

To look at the composition of L-valued relations in the case $L = 2(= \{\top, \bot\})$, consider $R \in \mathbf{Mat}(L)(X,Y)$ and $S \in \mathbf{Mat}(L)(Y,Z)$. Since joins and meets are defined by logical conjunctions and logical disjunctions, respectively, their composition is given as follows.

$$\begin{aligned} (S \circ R)(x,z) = \top \quad &\stackrel{\mathrm{def}}{\Longleftrightarrow} \bigvee\{\, S(y,z) \wedge R(x,y) \mid y \in Y \,\} = \top \\ &\Longleftrightarrow (\exists y \in Y) S(y,z) \wedge R(x,y) = \top \\ &\Longleftrightarrow (\exists y \in Y) S(y,z) = \top \text{ and } R(x,y) = \top \end{aligned}$$

It agrees with the composition of ordinary binary relations.

In the case $L = 2^n$ for some natural number n, an L-valued relation is regarded as a superposition of n ordinary binary relations whose state sets are identical. For example, an L-valued relation R for $L = \{\top, \bot\} \times \{\top, \bot\}$ is regarded as a superposition of 2-valued relations R_1 and R_2. Then, the first projection of $R(x,y)$ is $R_1(x,y)$ and the second one is $R_2(x,y)$.

The truth value should not be restricted to be finite. In software model checking, a state set is often infinite. For a fixed infinite state set, the number of models over it is of course infinite. So, we sometimes need a superposition of infinite models. So, our leading example of L is a powerset $\wp(M)$ with the inclusion order for an arbitrary set M. For example, a $\wp(M)$-valued relation R is regarded as the superposition of a family $(R_m)_{m \in M}$ of 2-valued relations such that $m \in R(x,y)$ if and only if $R_m(x,y) = \top$. Consider R and S as the

superposition of a family $(R_m)_{m\in M}$ and that of $(S_m)_{m\in M}$, respectively. Since the join of $\wp(M)$ is defined by the set-union, their composition is given as follows.

$$\begin{array}{ll} m \in (S \circ R)(x,z) & \stackrel{\text{def}}{\Longleftrightarrow} m \in \bigcup\{\, S(y,z) \cap R(x,y) \mid y \in Y \,\} \\ & \Longleftrightarrow (\exists y \in Y) m \in S(y,z) \cap R(x,y) \\ & \Longleftrightarrow (\exists y \in Y) m \in S(y,z) \text{ and } m \in R(x,y) \\ & \Longleftrightarrow (\exists y \in Y) S_m(y,z) = \top \text{ and } R_m(x,y) = \top \\ & \Longleftrightarrow (S_m \circ R_m)(x,z) = \top \end{array}$$

So, we can regard $S \circ R$ as the superposition of $(S_m \circ R_m)_{m\in M}$.

The set of all open sets in a topological space also form a frame with the inclusion order, since set-intersections distribute over set-unions. This example is important for our main theorem in Section 6.

Small sets and 2-valued binary relations inbetween form a typical *allegory*, a category with added structure. The added structure includes the operation sending $R\colon X \nrightarrow Y$ to $R^\circ\colon Y \nrightarrow X$ such that $R^\circ(y,x) \stackrel{\text{def}}{=} R(x,y)$. It is known that L-valued relations for an arbitrary frame L also form an allegory [5, 11] with R° defined similarly. In the rest of this paper, we use this operation.

3 Multi-Valued Kripke Structures and Simulation

In this section, we introduce the notion of multi-valued Kripke structure and simulations between them.

Definition 3.1 (L-Kripke structure)**.** Let L be a frame. Let **Atom** be a signature (a set of atomic propositions). An *L-valued Kripke structure (L-Kripke structure)* is a quadruplet of a set S, an L-valued relation $\rightarrow$ upon S, an L-valued relation $\rho\colon S \nrightarrow \mathbf{Atom}$, and an element I of $[S, L]$.

We write $s \rightarrow s'$ for the truth value $\rightarrow(s, s')$ in L hereafter.

When $L = 2$, an L-Kripke structure $K = (S, \rightarrow, \rho, I)$ corresponds to an ordinary Kripke structure where S gives the set of its states, $\rightarrow$ gives its transition relation, ρ gives its labelling function, and I gives the set of its initial states.

When $L = \wp(M)$, $(S, \rightarrow)$ can be seen as a superposition of a family of relations, as explained in Section 2. Similarly, ρ and I are also regarded as superpositions of a family $(\rho_m)_{m\in M}$ of labelling functions and a family $(I_m)_{m\in M}$ of initial states, respectively.

We extend the notion of simulation between ordinary Kripke structures to one between L-Kripke structures. In the standard context, a *simulation* from $A = (S_A, \rightarrow_A, \rho_A, I_A)$ to $C = (S_C, \rightarrow_C, \rho_C, I_C)$ is defined to be a relation $\Sigma \subseteq S_A \times S_C$ satisfying the following conditions. (1) If $\Sigma(a, c)$ and $c \rightarrow_C c'$, there is a state $a' \in S_A$ such that $\Sigma(a', c')$ and $a \rightarrow_A a'$. (2) If $\Sigma(a, c)$, the set of atomic propositions holding at c coincides with the set of atomic propositions holding at a. (3) If c is an initial state of C, then there is an initial state a of A

satisfying $\Sigma(a, c)$. Σ in Fig. 1 is an example of a simulation from A to C. Now, $\mathbf{Atom} = \{P\}$. C has four states and A has two. Σ relates a state of A to two states of C.

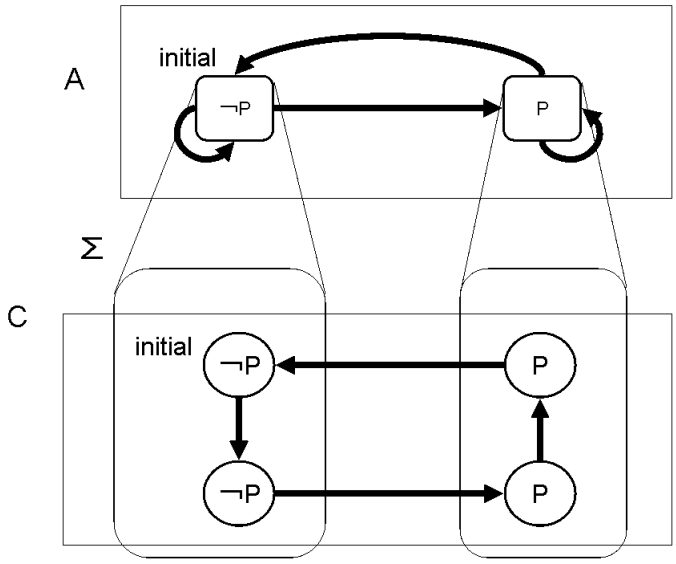
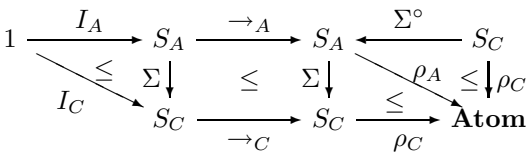


Figure 1: Example of Simulation

To extend the standard definition of simulations to one between L-Kripke structures naturally, we use the notion of locally ordered categories. A *locally ordered category* is a category whose homsets are equipped with partial orders and whose composition is order-preserving. Typical examples include the category of sets and relations. The standard definition of simulations can be stated in the locally ordered category [12, 10, 15]. The formulation can be applied to $\mathbf{Mat}(L)$ to obtain a definition of simulations there, since $\mathbf{Mat}(L)$ is also a locally ordered category whose homsets have pointwise orders. We define the notion of simulations between L-Kripke structures as follows. Here we regard $I \in [S, L]$ as an L-valued relation $I\colon\ 1 \longrightarrow S$ where 1 is the set with one element.

Definition 3.2 (Simulation)**.** Let $A = (S_A, \rightarrow_A, \rho_A, I_A)$ and $C = (S_C, \rightarrow_C, \rho_C, I_C)$ be L-Kripke structures. An L-valued relation $\Sigma\colon\ S_A \nrightarrow S_C$ is defined to be a *simulation* from A to C if and only if the following four conditions hold.

$$\begin{array}{rcl} \rightarrow_C \circ \Sigma & \leq & \Sigma \circ \rightarrow_A \\ \rho_C \circ \Sigma & \leq & \rho_A \\ \rho_A \circ \Sigma^{\circ} & \leq & \rho_C \\ I_C & \leq & \Sigma \circ I_A \end{array}$$



The first condition says that for any $c, c' \in S_C$ and $a \in S_A$, $(c \to_C c') \wedge \Sigma(a, c) \leq \vee\{\Sigma(a', c') \wedge (a \to_A a') \mid a' \in S_A\}$ holds. When $L = 2$, this means, if $\Sigma(a, c)$ and $c \to_C c'$, then there is a state $a' \in S_A$ such that $\Sigma(a', c')$ and $a \to_A a'$.

The second condition says that for any $P \in \mathbf{Atom}$, $c \in S_C$ and $a \in S_A$, $\rho_C(c, P) \wedge \Sigma(a, c) \leq \rho_A(a, P)$ holds. The third condition says that for any $P \in \mathbf{Atom}$, $c \in S_C$ and $a \in S_A$, $\rho_A(a, P) \wedge \Sigma(a, c) \leq \rho_C(c, P)$ holds. When $L = 2$, these two conditions mean, if $\Sigma(a, c)$ then the set of atomic propositions holding at c coincides with the set of atomic propositions holding at a.

The fourth condition says that for any $c \in S_C$ and $a \in S_A$, $I_C(c) \leq \vee\{\Sigma(a, c) \wedge I_A(a) \mid a \in S_A\}$ holds. When $L = 2$, this means, if c is an initial state of C, then there is an initial state a of A satisfying $\Sigma(a, c)$.

When $L = \wp(M)$, the compositions of L-valued relations can be interpreted for each m, as explained in Section 2. So, a simulation between L-Kripke structures is regarded as a superposition of a family of simulations indexed by M.

As far as the authors know, this is the first definition of multi-valued simulations.

Simulations have been used in model checking in order to solve the state explosion problem, since when there is a simulation from a smaller model A to a larger one C, in order to check some property on C, it is sufficient to check it on A. This theorem is called the *simulation theorem*. In the rest of this paper, we discuss a sufficient condition to make the theorem hold.

4 Multi-Valued Models for Modal μ-Calculus

In this section, we define the models of an intuitionistic variant of modal μ-calculus over multi-valued Kripke structures, and formulate and prove the simulation theorem in this context.

Propositional modal μ-calculus [13] is a powerful logic equipped with modalities and the least and greatest fixpoints. One of its application domain is to describe temporal specifications for model checking. In this section, we give the notion of model for modal μ-calculus in terms of L-Kripke structures.

We shall define the formulae of modal μ-calculus by extending those of intuitionistic modal logic [16] with the least and greatest fixpoints. Here, we do not follow the standard definition of modal μ-formulae found in e.g. Kozen's paper [13], since we will be giving an intuitionistic interpretation in which $(\Diamond\varphi) \Leftrightarrow (\neg\Box\neg\varphi)$ and $(\varphi \Rightarrow \psi) \Leftrightarrow (\neg\varphi \vee \psi)$ do not necessarily hold, and we must, therefore, have $\Rightarrow$ and $\Diamond$ as primitives. Let **Atom** be a signature (a set of atomic propositions), and **Var** be the set of propositional variables.

Definition 4.1 (Intuitionistic modal μ-formulae)**.** *Intuitionistic modal μ-formulae* are generated by the following grammar where $P \in \mathbf{Atom}$, $X \in \mathbf{Var}$, and the grammar is subject to the side condition that both of $\mu X.\varphi$ and $\nu X.\varphi$ have no free negative occurrences of X in φ.

$$\begin{array}{rcl} \varphi & ::= & P \mid X \mid \mu X.\varphi \mid \nu X.\varphi \mid \Box\varphi \mid \Diamond\varphi \mid \varphi \Rightarrow \varphi \\ & \mid & \bot \mid \top \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \end{array}$$

The operator $\Rightarrow$ represents implication. $\Box$ and $\Diamond$ are modal operators. Operators μ and ν represent the least fixed point and the greatest fixed point, respectively. It is known that under the standard interpretation modal μ-calculus is strictly expressive than computational tree logic (CTL) [2], one of the standard temporal logic. For example, the formula $\nu X.P \wedge \Box X$ expresses the CTL formula $\mathbf{AG}P$.

Definition 4.2. Let L be a frame, $K = (S, \to, \rho, I)$ be an L-Kripke structure, and V be a valuation of variables (i.e., a function $V\colon \mathbf{Var} \longrightarrow [S, L]$). We define the *truth value* $[\![\varphi]\!]_{K,V} \in [S, L]$ of a intuitionistic modal μ-formula φ inductively as follows.

$$\begin{array}{lcl} [\![P]\!]_{K,V}(s) & \stackrel{\text{def}}{=} & \rho(s, P) \\ [\![X]\!]_{K,V} & \stackrel{\text{def}}{=} & V(X) \\ [\![\mu X.\varphi]\!]_{K,V} & \stackrel{\text{def}}{=} & \bigwedge\{\, W \in [S, L] \mid [\![\varphi]\!]_{K,V[X\mapsto W]} \leq W \,\} \\ [\![\nu X.\varphi]\!]_{K,V} & \stackrel{\text{def}}{=} & \bigvee\{\, W \in [S, L] \mid W \leq [\![\varphi]\!]_{K,V[X\mapsto W]} \} \\ [\![\Box\varphi]\!]_{K,V}(s) & \stackrel{\text{def}}{=} & \bigwedge\{\, (s \to t) \Rightarrow [\![\varphi]\!]_{K,V}(t) \mid t \in S \,\} \\ [\![\Diamond\varphi]\!]_{K,V}(s) & \stackrel{\text{def}}{=} & \bigvee\{\, (s \to t) \wedge [\![\varphi]\!]_{K,V}(t) \mid t \in S \,\} \end{array}$$

Here, $V[X \mapsto W]$ denotes the valuation which sends X to W and the other variable Y to $V(Y)$. Operators $\Rightarrow$, $\bot$, $\top$, $\vee$, and $\wedge$ are interpreted by the corresponding structure of the frame L. Moreover, we write $K \models_{\mathbf{State}} \varphi$ (φ is *valid in* K) if and only if $I \leq [\![\varphi]\!]_{K,V}$ holds for any valuation V.

When $L = 2$, the above truth value agrees with the standard one introduced by Kozen [13]. For example, modal operators satisfy

$$\begin{array}{rcl} [\![\Box\varphi]\!]_{K,V}(s) = \top & \stackrel{\text{def}}{\Longleftrightarrow} & \bigwedge\{\, (s \to t) \Rightarrow [\![\varphi]\!]_{K,V}(t) \mid t \in S \,\} = \top \\ & \Longleftrightarrow & (\forall t \in S)\, (s \to t) \Rightarrow [\![\varphi]\!]_{K,V}(t) = \top \\ & \Longleftrightarrow & (\forall t \in S) \text{ if } (s \to t) = \top \text{ then } [\![\varphi]\!]_{K,V}(t) = \top \end{array}$$

and

$$\begin{array}{rcl} [\![\Diamond\varphi]\!]_{K,V}(s) = \top & \stackrel{\text{def}}{\Longleftrightarrow} & \bigvee\{\, (s \to t) \wedge [\![\varphi]\!]_{K,V}(t) \mid t \in S \,\} = \top \\ & \Longleftrightarrow & (\exists t \in S)\, (s \to t) \wedge [\![\varphi]\!]_{K,V}(t) = \top \\ & \Longleftrightarrow & (\exists t \in S)\, (s \to t) = \top \text{ and } [\![\varphi]\!]_{K,V}(t) = \top. \end{array}$$

Moreover, the validity in the Kripke structure satisfies

$$\begin{array}{rcl} K \models_{\mathbf{State}} \varphi & \stackrel{\text{def}}{\Longleftrightarrow} & (\forall V)\, I \leq [\![\varphi]\!]_{K,V} \\ & \Longleftrightarrow & (\forall V)(\forall s \in S)\, I(s) \leq [\![\varphi]\!]_{K,V}(s) \\ & \Longleftrightarrow & (\forall V)(\forall s \in S) \text{ if } I(s) = \top \text{ then } [\![\varphi]\!]_{K,V}(s) = \top \\ & \Longleftrightarrow & (\forall V)(\forall s\colon \text{ initial state})[\![\varphi]\!]_{K,V}(s) = \top. \end{array}$$

When $L = \wp(M)$, an L-Kripke structure K is regarded as a superposition of a family $(K_m)_{m\in M}$ of ordinary Kripke structures, as explained in Section 3. The above truth value is a natural generalisation of 2-valued one, since we have $m \in [\![\varphi]\!]_{K,V} \Longleftrightarrow [\![\varphi]\!]_{K_m,V} = \top$. Moreover, the validity also satisfies

$$K \models_{\mathbf{State}} \varphi \Longleftrightarrow (\forall m \in M) K_m \models_{\mathbf{State}} \varphi.$$

As L is a frame, this definition of truth values gives an intuitionistic interpretation. However, when L would moreover be a complete Boolean algebra, i.e., if $((x \Rightarrow \bot) \Rightarrow \bot) = x$ for each x, then this automatically would give a classical interpretation, i.e., double negation could be eliminated and the de Morgan duality would hold.

We formulate the simulation theorem for the above semantics. The simulation theorem for ordinary Kripke models states that, the truth of universal formulae (including ACTL* formulae) is preserved by a simulation [14]. We can show that the same theorem holds for L-Kripke models.

Definition 4.3 ($\Box L\mu$ formulae)**.** $\Box L\mu$ *formulae* are intuitionistic modal μ-formulae with no negative occurrences of subformulae of the form $\Box\psi$ and no positive occurrences of subformulae of the form $\Diamond\psi$.

For example, $\Diamond P \Rightarrow \Box P$ is a $\Box L\mu$ formula.

Theorem 4.4 (Simulation Theorem)**.** Let A and C be L-Kripke structures and assume that there is a simulation from A to C. For an arbitrary $\Box L\mu$ formula φ with no free variables, $A \models_{\mathbf{State}} \varphi$ implies $C \models_{\mathbf{State}} \varphi$.

This statement can be generalised for formulae with free variables. It can be proved by the structural induction on formulae. See Appendix A for the details. The case $L = 2$ reduces to the standard simulation theorem.

5 Path Model Construction

Linear-time temporal logic (LTL) [17] and computational tree logic (CTL) [2] are temporal logics intensively used for model-checking. While the formulae of CTL and those of modal μ-calculus are *state formulae* whose validity in a model is defined by truth in all initial states, the formulae of LTL are *path formulae* whose validity in a model is defined by truth in all the paths starting from the initial states. In this section, we regard the intuitionistic modal μ-formulae as path formulae and define their validity with respect to paths of an L-Kripke structure.

A *path* in an L-Kripke structure $K = (S, \rightarrow, \rho, I)$ is an infinite (countable) sequence of states. We write ω for the set of all natural numbers and $[\omega, S]$ for the set of all paths. In the context of ordinary Kripke structures, an infinite sequence σ of states is defined to be a real path, if each of its states is related to the next state by the transition: $(\sigma(n) \rightarrow \sigma(n+1)) = \top$. In our context, however, a transition may have an intermediate degree which is neither $\top$ nor $\bot$.

It is not natural to regard only the sequences related by $\top$ as real paths. Hence we should take into account all sequences together with how deeply their states are related by the transition. We define $\mathbf{Weight}(K) \in [[\omega, S], L]$ as follows.

$$\mathbf{Weight}(K)(\sigma) \stackrel{\text{def}}{=} \bigwedge_{n \in \omega} (\sigma(n) \to \sigma(n+1))$$

When $L = 2$, $\mathbf{Weight}(K)(\sigma) = \top$ if and only if σ is a real path in K. When $L = \wp(M)$, an L-Kripke structure K is regarded as a superposition of $(K_m)_{m \in M}$. It satisfies the following.

$$m \in \mathbf{Weight}(K)(\sigma) \Longleftrightarrow \mathbf{Weight}(K_m)(\sigma) = \top$$

So, $m \in \mathbf{Weight}(K)(\sigma)$ if and only if σ is a real path in K_m.

Given an L-Kripke structure, one can construct another L-Kripke structure based on the paths of the original structure as follows. We call this construction *path model construction*.

Definition 5.1 (Path Model Construction)**.** Let L be a frame and $K = (S, \to, \rho, I)$ be an L-Kripke structure. We define an L-Kripke structure $\mathbf{Path}(K)$ by $(S', \to', \rho', I')$ where

- $S' \stackrel{\text{def}}{=} [\omega, S]$, i.e., the set of all infinite (countable) sequences of elements of S,
- $\sigma \to' \tau \stackrel{\text{def}}{=} \begin{cases} \top & \text{if } \tau(n) = \sigma(n+1) \text{ for all } n \in \omega, \\ \bot & \text{otherwise,} \end{cases}$
- $\rho'(\sigma, P) \stackrel{\text{def}}{=} \rho(\sigma(0), P)$, and
- $I'(\sigma) \stackrel{\text{def}}{=} I(\sigma(0)) \wedge \mathbf{Weight}(K)(\sigma)$.

Note that for all $\sigma \in S'$, there exists a unique $\tau \in S'$ such that $\sigma \to' \tau = \top$ (of course $\tau = \sigma(1)\sigma(2)\cdots$). Therefore, we have $[\![\Diamond\varphi]\!]_{\mathbf{Path}(K),V} = [\![\Box\varphi]\!]_{\mathbf{Path}(K),V}$.

When $L = 2$, an initial state of $\mathbf{Path}(K)$ corresponds to a real path starting from initial states of K. All reachable states from the initial states of $\mathbf{Path}(K)$ are real paths of K, since $\sigma \to' \tau = \top$ and $\mathbf{Weight}(K)(\sigma) = \top$ imply $\mathbf{Weight}(K)(\tau) = \top$. For example, consider the Kripke structure K and $\mathbf{Path}(K)$ in Fig. 2. Reachable states from the initial state in $\mathbf{Path}(K)$ are $abbb\cdots$ and $bbb\cdots$. They are real paths in K. States in $\mathbf{Path}(K)$ include $aabbb\cdots$, which is not a real path in K. So, it is not reachable from the initial state in $\mathbf{Path}(K)$.

When $L = \wp(M)$, $\mathbf{Path}(K)$ is regarded as a superposition of $(K_m)_{m \in M}$ by the following reason. The state set of $\mathbf{Path}(K)$ is the same as that of $\mathbf{Path}(K_m)$ for each $m \in M$. The transition of $\mathbf{Path}(K)$ is also equal to that of $\mathbf{Path}(K_m)$ for each $m \in M$, since they are independent of the transition of K or that of K_m. For the labelling function, $m \in \rho'(\sigma, P)$ is logically equivalent to $\rho_m(\sigma(0), P) = \top$. The initial states satisfy $m \in I'(\sigma) \Longleftrightarrow I'_m(\sigma) = \top$.

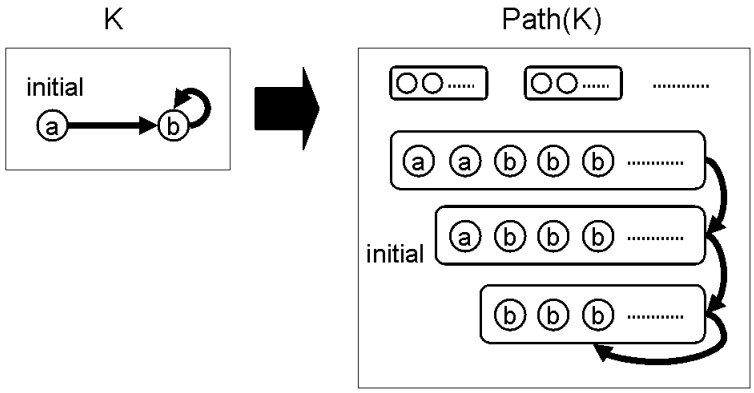


Figure 2: Example of Path Model Construction

The path model construction allows us to consider the validity of an intuitionistic modal μ-formula with respect to paths as follows.

Definition 5.2 (Validity in Path Model)**.** For an intuitionistic modal μ-formula φ and an L-Kripke structure K, we write $K \models_{\mathbf{Path}} \varphi$ if and only if φ is valid in $\mathbf{Path}(K)$.

When $L = 2$, the above validity is the natural extension of the validity of LTL formulae in the standard path semantics [3], that is to say, that φ is true in all the real paths starting from initial states of K, provided the transition relation of K is total.

6 Simulation Lifting

In this section, we investigate the simulation theorem for path models. The theorem to be proved is that if there is a simulation from A to C, then $A \models_{\mathbf{Path}} \varphi$ implies $C \models_{\mathbf{Path}} \varphi$ for an arbitrary intuitionistic modal μ-formula φ. Here, φ can be translated into the $\Box L\mu$ formula that has the same validity, since every intuitionistic modal μ-formula ψ satisfies $[\![\Diamond\psi]\!]_{\mathbf{Path}(K),V} = [\![\Box\psi]\!]_{\mathbf{Path}(K),V}$.

For the simulation theorem to hold, it suffices if, given a simulation from A to C, we can construct a simulation from $\mathbf{Path}(A)$ to $\mathbf{Path}(C)$, since we have:

$$\begin{array}{ll} & A \models_{\mathbf{Path}} \varphi \\ \iff & \mathbf{Path}(A) \models_{\mathbf{State}} \varphi \\ \implies & \mathbf{Path}(C) \models_{\mathbf{State}} \varphi \quad \text{(by Theorem 4.4)} \\ \iff & C \models_{\mathbf{Path}} \varphi. \end{array}$$

An L-relation $\Sigma\colon S_A \nrightarrow S_C$ is naturally lifted to the L-relation $\Sigma'\colon S'_A \nrightarrow S'_C$ such that $\Sigma'(\sigma,\tau) = \bigwedge_{i\in\omega} \Sigma(\sigma(i),\tau(i))$. One may expect that, when Σ is a

simulation, then Σ' is also a simulation. However, it does not always hold. What is even worse, we have L, A and C such that there exists no simulation from $\mathbf{Path}(A)$ to $\mathbf{Path}(C)$ while there is a simulation from A to C.

Example (Counterexample of Simulation Lifting): Let $\mathbf{R}$ be the set of all real numbers. For all $p, q \in \mathbf{R}$ such that $p < q$, we write (p, q) for $\{r \in \mathbf{R} \mid p < r < q\}$. Let L be the set of all open sets of the standard topology on $\mathbf{R}$. L is a frame, as mentioned in Section 2. We construct L-Kripke structures A, C, and a simulation Σ such that there is no simulation from $\mathbf{Path}(A)$ to $\mathbf{Path}(C)$. Let C be the L-Kripke structure such that $S_C = \{*\}$, $I_C = \top$, $\rho_C = \top$, and $* \to_C * = \top$. Let A be the L-Kripke structure such that $S_A = \{(p, q) \mid p, q \in \mathbf{R},\ p < q\}$, $I_A = \top$, $\rho_A = \top$, and $(p, q) \to_A x = x$ if $x = (p, \frac{p+2q}{3})$ or $x = (\frac{2p+q}{3}, q)$, and $(p, q) \to_A x = \bot$ otherwise.

Let $\Sigma\colon S_A \nrightarrow S_C$ be $\Sigma(x, *) = x$. Σ is a simulation from A to C, since $\rho_C \circ \Sigma \leq \rho_A$, $\rho_A \circ \Sigma^\circ \leq \rho_C$, and $I_C \leq \Sigma \circ I_A$ are trivial, and the rest is proved by

$$
\begin{array}{ll}
 & \to_C \circ \Sigma \leq \Sigma \circ \to_A \\
\iff & (* \to_C *) \cap \Sigma(x, *) \subseteq \cup\{\Sigma(x', *) \cap (x \to_A x') \mid x' \in S_A\}, \text{ for all } x \in S_A \\
\iff & x \subseteq \cup\{x' \in S_A \mid x \to_A x' = x'\}, \text{ for all } x \in S_A \\
\iff & (p, q) = (p, \frac{p+2q}{3}) \cup (\frac{2p+q}{3}, q), \text{ for all } (p, q) \in S_A.
\end{array}
$$

However, there exists no simulation from $\mathbf{Path}(A)$ to $\mathbf{Path}(C)$, since $I'_C = \top$ but $I'_A = \bot$. The point is that L is not closed under countable set-intersection, that is to say, the operation $\bigwedge_{n\in\omega}$ in L is different from the countable set-intersection. For all $\alpha \in S'_A$, $\bigwedge_{n\in\omega}(\alpha(n) \to \alpha(n+1))$ is always $\bot$, but $\bigcap_{n\in\omega}(\alpha(n) \to \alpha(n+1))$ is not so.

Here, we give a sufficient condition on the frame L for which our path model construction lifts simulations. This sufficient condition implies that $\bigwedge_{n\in\omega}$ coincides with $\bigcap_{n\in\omega}$.

Proposition 6.1. Let L be a frame isomorphic to the open sets of a topological space which is closed under countable intersections. Let A and C be L-Kripke structures. If there is a simulation from A to C, then there is a simulation from $\mathbf{Path}(A)$ to $\mathbf{Path}(C)$.

Proof. Let Σ be a simulation from A to C. We write $\mathbf{Path}(A) = (S'_A, \to'_A, \rho'_A, I'_A)$ and $\mathbf{Path}(C) = (S'_C, \to'_C, \rho'_C, I'_C)$. We define $\Sigma'\colon S'_A \nrightarrow S'_C$ by $\Sigma'(\sigma, \tau) = \bigwedge_{i\in\omega} \Sigma(\sigma(i), \tau(i))$ and prove that it is a simulation from $\mathbf{Path}(A)$ to $\mathbf{Path}(C)$.

To show $\to'_C \circ \Sigma' \leq \Sigma' \circ \to'_A$, it is sufficient to show that for all $\alpha \in S'_A$, $\beta, \gamma \in S'_C$, there is a $\delta \in S'_A$ such that $(\gamma \to'_C \beta) \cap \Sigma'(\alpha, \gamma) \subseteq \Sigma'(\delta, \beta) \cap (\alpha \to'_A \delta)$. Take as δ the sequence $\alpha(1)\alpha(2)\alpha(3)\cdots$. Assume that β satisfies $\gamma \to'_C \beta = \top$. Then, β must be $\gamma(1)\gamma(2)\cdots$ and they satisfy

$$\Sigma'(\alpha, \gamma) = \bigcap_{n\in\omega} \Sigma(\alpha(n), \gamma(n)) \subseteq \bigcap_{n\in\omega} \Sigma(\alpha(n+1), \gamma(n+1)) = \Sigma'(\delta, \beta).$$

Therefore, the statement is proved.

To show $\rho'_C \circ \Sigma' \leq \rho'_A$, it is sufficient to show that all $\alpha \in S'_A$, $\gamma \in S'_C$, and $P \in \mathbf{Atom}$ satisfy $\rho'_C(\gamma, P) \cap \Sigma'(\alpha, \gamma) \subseteq \rho'_A(\alpha, P)$. Since Σ is a simulation,

$$\rho_C(\gamma(0), P) \cap \Sigma'(\alpha, \gamma) \subseteq \rho_C(\gamma(0), P) \cap \Sigma(\alpha(0), \gamma(0)) \subseteq \rho_A(\alpha(0), P).$$

Similarly, $\rho'_A \circ \Sigma'^{\circ} \leq \rho'_C$ is also proved.

To show $I'_C \leq \Sigma' \circ I'_A$, it is sufficient to show that all $\gamma \in S'_C$ satisfy

$$\begin{array}{ll} & I_C(\gamma(0)) \cap \bigcap_{n\in\omega}(\gamma(n) \rightarrow_C \gamma(n+1)) \\ \subseteq & \bigcup\{I_A(\alpha(0)) \cap \bigcap_{n\in\omega}(\alpha(n) \rightarrow_A \alpha(n+1)) \cap \bigcap_{n\in\omega} \Sigma(\alpha(n), \gamma(n)) \mid \alpha \in S'_A\}. \end{array}$$

Let s be an element of the left-hand side. By $I_C \leq \Sigma \circ I_A$, we have $I_C(\gamma(0)) \subseteq \bigcup\{\Sigma(a, \gamma(0)) \cap I_A(a) \mid a \in S_A\}$. Since $s \in I_C(\gamma(0))$, there is an $a_0 \in S_A$ such that $s \in \Sigma(a_0, \gamma(0)) \cap I_A(a_0)$. By $\rightarrow_C \circ \Sigma \leq \Sigma \circ \rightarrow_A$, we have $(\gamma(0) \rightarrow_C \gamma(1)) \cap \Sigma(a_0, \gamma(0)) \subseteq \bigcup\{(a_0 \rightarrow_A a') \cap \Sigma(a', \gamma(1)) \mid a' \in S_A\}$. Since $s \in (\gamma(0) \rightarrow_C \gamma(1))$, there is an $a_1 \in S_A$ such that $s \in (a_0 \rightarrow_A a_1) \cap \Sigma(a_1, \gamma(1))$. Similarly, for any $n \in \omega$, we can always choose an appropriate $a_n \in S_A$ such that $s \in (a_n \rightarrow_A a_{n+1}) \cap \Sigma(a_n, \gamma(n))$. By countable choice we can construct a path α which consists of $a_0, a_1, a_2, \cdots$. Therefore, the statement is proved. □

Our sufficient condition is general enough to cover most examples of frames that appear in practice. For example, when $L = \wp(S)$ for some set S, it is the discrete topology on S, which is closed under countable set-intersections. By the representation theorem [18], all atomic complete Boolean algebras also satisfy the condition. All finite frames are trivial examples. $L = \omega + 1 = \omega \cup \{\omega\}$ is another example. By interpreting $\alpha \in L$ as $\{n \in \omega \mid n < \alpha\}$, it forms a topology on ω, which is closed under countable set-intersections.

Now, the simulation theorem for the validity in path models can be formulated as follows.

Theorem 6.2 (Simulation Theorem for Path Model)**.** Let L be a frame isomorphic to the open sets of a topological space which are closed under countable intersections. Let A and C be L-Kripke structures and assume that there is a simulation from A to C. For an arbitrary intuitionistic modal μ-formula φ with no free variables, $A \models_{\mathbf{Path}} \varphi$ implies $C \models_{\mathbf{Path}} \varphi$.

Proof. Proposition 6.1 and Theorem 4.4 imply this theorem. □

7 Related Work

In this section, we compare our work with related work.

Fitting takes finite Heyting algebra to be the structure of truth values in his formulation of the many-valued Kripke models for propositional modal logic [4]. His motivation is to superpose a family of Kripke models with a domination order among models. He mentions that the result can be extended to complete Heyting algebra (that is, frame). Our result can be seen as extending his logic with fixed point operators and the notion of simulation.

In the context of model checking, Chechik, Gurfinkel and others generalise semantics of modal μ-calculus based on de Morgan algebra [1, 8]. A *de Morgan algebra* is a structure $(L, \vee, \wedge, \bot, \top, \neg)$, where $(L, \vee, \wedge, \bot, \top)$ is a finite distributive bounded lattice (i.e., finite frame) and $\neg\colon L \longrightarrow L$ satisfies $\neg\neg x = x$ and de Morgan laws: $\neg(x \wedge y) = \neg x \vee \neg y$, and $\neg(x \vee y) = \neg x \wedge \neg y$. Since a de Morgan algebra is also a finite frame, our definition of frame-valued truth values is applicable to the case of de Morgan algebras. As mentioned in the paper [8], however, they give a different truth value for $\Box\varphi$ from Fitting's truth value (that is, our truth value) as follows.

$$[\![\Box\varphi]\!]_{K,V}(s) \stackrel{\text{def}}{=} \bigwedge\{\, \neg(s \to t) \vee [\![\varphi]\!]_{K,V}(t) \mid t \in S \,\}.$$

The truth value satisfies $\Diamond\neg\varphi = \neg\Box\varphi$ and does not satisfy $\Diamond\varphi \wedge \Box\psi \leq \Diamond(\varphi \wedge \psi)$. On the other hand, our truth value satisfies $\Diamond\varphi \wedge \Box\psi \leq \Diamond(\varphi \wedge \psi)$ and does not satisfy $\Diamond(\varphi \Rightarrow \bot) = \Box\varphi \Rightarrow \bot$. Therefore, our work and the work by Chechik, Gurfinkel and others are orthogonal.

8 Conclusion

We have proved two simulation theorems for multi-valued modal μ-calculus. One is based on multi-valued Kripke models, whose truth value is defined over an arbitrary complete Heyting algebra. The other is based on multi-valued path models. The second one does not hold for the truth value defined over an arbitrary complete Heyting algebra. We also gave a sufficient condition to make it hold. To our knowledge, this is the first work on investigating the sufficient conditions for the simulation theorem in the context of multi-valued Kripke structures and multi-valued simulation relations.

It is left for future work to account for fuzzy relations [7, 6, 11] and probabilistic temporal logics [9] by extending our framework. Another interesting topic to be studied is categorical semantics of intuitionistic modal μ-calculus. It will allow us to consider models other than $\mathbf{Mat}(L)$. From the practical side, developing an efficient model checking algorithm with respect to our multi-valued models also needs to be addressed.

Acknowledgments

We would like to thank Ko Sakai for many valuable discussions during this research. Comments by John Power and Hitoshi Furusawa are also gratefully acknowledged.

References

[1] Marsha Chechik, Benet Devereux, Steve M. Easterbrook, Albert Y. C. Lai, and Victor Petrovykh. Efficient multiple-valued model-checking using lattice representations. In *CONCUR*, pages 441–455, 2001.

[2] Edmund M. Clarke and E. Allen Emerson. Design and synthesis of synchronization skeletons using branching-time temporal logic. In *Logic of Programs*, pages 52–71, 1981.

[3] Edmund M. Clarke, Orna Grumberg, and Doron A. Peled. *Model Checking*. The MIT Press, Cambridge, Massachusetts, 1999.

[4] Melvin C. Fitting. Many-valued modal logics II. *Fundamenta Informaticae*, XVII:55–74, 1992.

[5] Peter J. Freyd and Andre Scedrov. *Categories, Allegories*, volume 39 of *North-Holland Mathematical Library*. North-Holland, Amsterdam, 1990.

[6] Hitoshi Furusawa. *Algebraic Formalisations of Fuzzy Relations and Their Representation Theorems*. PhD thesis, Department of Informatics, Kyushu University, March 1998.

[7] J. A. Goguen. L-fuzzy sets. *Journal of Mathematical Analysis and Applications*, 18:145–174, 1967.

[8] Arie Gurfinkel and Marsha Chechik. Multi-valued model checking via classical model checking. In Roberto M. Amadio and Denis Lugiez, editors, *CONCUR*, volume 2761 of *Lecture Notes in Computer Science*, pages 263–277. Springer, 2003.

[9] Hans Hansson and Bengt Jonsson. A logic for reasoning about time and reliability. *Formal Aspects of Computing*, 6(5):512–535, 1994.

[10] Claudio Hermida. A categorical outlook on relational modalities and simulations. In Michael Mendler, Rajeev P. Goré, and Valeria de Paiva, editors, *Intuitionistic Modal Logic and Aplications*, volume 02-15 of *DIKU technical reports*, pages 17–34, July 26 2002.

[11] P. T. Johnstone. *Sketches of an Elephant: A Topos Theory Compendium*. Oxford Science Publications, 2002.

[12] Yoshiki Kinoshita and John Power. A general completeness result in refinement. In *WADT'99*, LNCS 1827, Springer Verlag, 2000.

[13] D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.

[14] Claire Loiseaux, Susanne Graf, Joseph Sifakis, Ahmed Bouajjani, and Saddek Bensalem. Property preserving abstractions for the verification of concurrent systems. *Formal Methods in System Design*, 6(1):11–44, 1995.

[15] Koki Nishizawa and Makoto Takeyama. Algebraic structure for a fixed point logic and abstract interpretation. Programming Science Technical Report AIST-PS-2005-012, Research Center of Verification and Semantics, National Institute of Advanced Industrial Science and Technology, February 2005.

[16] Plotkin and Stirling. A framework for intuitionistic modal logics (extended abstract). *TARK: Theoretical Aspects of Reasoning about Knowledge*, 1986.

[17] A. Pnueli. The temporal logic of programs. In *Proceedings of the Eighteenth Symposium on the Foundations of Computer Science*, pages 46–57, 1977.

[18] A. Tarski. Zur Grundlegung der Booleschen Algebra. *Fundamenta Mathematicae*, 24:177–198, 1935.

A A proof of Theorem 4.4

In this appendix, we prove Theorem 4.4. For that, we define some notions and generalise the theorem for formulae with free variables.

First, we define the dual notion of $\Box L\mu$ formula.

Definition A.1. $\Diamond L\mu$ *formulae* are intuitionistic modal μ-formulae with no negative occurrences of subformulae of the form $\Diamond\psi$ and no positive occurrences of subformulae of the form $\Box\psi$.

For example, $\Diamond P \Rightarrow \Box P$ and $\Box P \Rightarrow \Diamond P$ are a $\Box L\mu$ formula and a $\Diamond L\mu$ formula, respectively. An atomic proposition is an example of both. $\Box\Diamond P$ is neither a $\Box L\mu$ formula nor a $\Diamond L\mu$ formula. If $\varphi \Rightarrow \psi$ is a $\Box L\mu$ formula, then φ is a $\Diamond L\mu$ formula and ψ is a $\Box L\mu$ formula. If $\varphi \Rightarrow \psi$ is a $\Diamond L\mu$ formula, then the dual statement holds.

Next, we define the following notions in order to differently deal with free positive occurrences and free negative occurrences of variables.

Definition A.2. For an intuitionistic modal μ-formula ψ, $\mathbf{Pos}(\psi)$ denotes the set of variables which have free positive occurrences in ψ. $\mathbf{Neg}(\psi)$ denotes the set of variables which have free negative occurrences in ψ.

For example, $\mathbf{Pos}(X \Rightarrow Y)$ denotes $\{Y\}$ and $\mathbf{Neg}(X \Rightarrow Y)$ denotes $\{X\}$. Remark that $\mathbf{Pos}(\psi) \cap \mathbf{Neg}(\psi)$ is not always empty, for example, when $\psi = (X \wedge Y) \Rightarrow (X \wedge Z)$.

The following lemma generalises Theorem 4.4 for formulae with free variables.

Lemma A.3. Let A and C be L-Kripke structures, Σ be a simulation from A to C, and V_A and V_C, respectively, be a valuation of A and C, respectively.

Let ψ be a $\Box L\mu$ formula. If $\Sigma \circ V_A(X) \leq V_C(X)$ holds for every $X \in \mathbf{Pos}(\psi)$, and $\Sigma^\circ \circ V_C(Y) \leq V_A(Y)$ holds for every $Y \in \mathbf{Neg}(\psi)$, then we have $\Sigma \circ [\![\psi]\!]_{A,V_A} \leq [\![\psi]\!]_{C,V_C}$.

Let φ be a $\Diamond L\mu$ formula. If $\Sigma^\circ \circ V_C(X) \leq V_A(X)$ holds for every $X \in \mathbf{Pos}(\varphi)$, and $\Sigma \circ V_A(Y) \leq V_C(Y)$ holds for every $Y \in \mathbf{Neg}(\varphi)$, then we have $\Sigma^\circ \circ [\![\varphi]\!]_{C,V_C} \leq [\![\varphi]\!]_{A,V_A}$.

Proof. It is proved by simultaneous induction on ψ and φ.

(case $\psi = P$) To show $\Sigma \circ [\![P]\!]_{A,V_A} \leq [\![P]\!]_{C,V_C}$ is equivalent to show $\Sigma(a,c) \wedge \rho_A(a,P) \leq \rho_C(c,P)$ for every state a of A and every state c of C. It is implied by the condition $\rho_A \circ \Sigma^\circ \leq \rho_C$ of simulation Σ.

(case $\psi = X$) Since $X \in \mathbf{Pos}(\psi)$, we have $\Sigma \circ V_A(X) \leq V_C(X)$. That is equivalent to $\Sigma \circ [\![X]\!]_{A,V_A} \leq [\![X]\!]_{C,V_C}$.

(case $\psi = \mu X.\psi'$) We define $W(a) \stackrel{\text{def}}{=} \bigwedge\{\Sigma(a,c) \Rightarrow [\![\mu X.\psi']\!]_{C,V_C}(c) \mid c \in C\}$ for every state a of A. ψ' is a $\Box L\mu$ formula. $\Sigma \circ V_A[X \mapsto W](Y) \leq V_C[X \mapsto [\![\mu X.\psi']\!]_{C,V_C}](Y)$ holds for every $Y \in \mathbf{Pos}(\psi')$ and $\Sigma^\circ \circ V_C[X \mapsto [\![\mu X.\psi']\!]_{C,V_C}](Y) \leq V_A[X \mapsto W](Y)$ holds for every $Y \in \mathbf{Neg}(\psi')$. By induction hypothesis, we have $\Sigma \circ [\![\psi']\!]_{A,V_A[X\mapsto W]} \leq [\![\psi']\!]_{C,V_C[X\mapsto [\![\mu X.\psi']\!]_{C,V_C}]}$.

To show $\Sigma \circ [\![\mu X.\psi']\!]_{A,V_A} \leq [\![\mu X.\psi']\!]_{C,V_C}$ is equivalent to show $\Sigma(a,c) \wedge [\![\mu X.\psi']\!]_{A,V_A}(a) \leq [\![\mu X.\psi']\!]_{C,V_C}(c)$ for every state a of A and every state c of C. It is proved as follows.

$$
\begin{array}{ll}
 & \forall a \in A, \forall c \in C, \Sigma(a,c) \wedge [\![\mu X.\psi']\!]_{A,V_A}(a) \leq [\![\mu X.\psi']\!]_{C,V_C}(c) \\
\iff & \forall a \in A, \forall c \in C, [\![\mu X.\psi']\!]_{A,V_A}(a) \leq \Sigma(a,c) \Rightarrow [\![\mu X.\psi']\!]_{C,V_C}(c) \\
\iff & [\![\mu X.\psi']\!]_{A,V_A} \leq W \\
\Longleftarrow & [\![\psi']\!]_{A,V_A[X\mapsto W]} \leq W \\
\iff & \forall a \in A, \forall c \in C, [\![\psi']\!]_{A,V_A[X\mapsto W]}(a) \leq \Sigma(a,c) \Rightarrow [\![\mu X.\psi']\!]_{C,V_C}(c) \\
\iff & \forall a \in A, \forall c \in C, \Sigma(a,c) \wedge [\![\psi']\!]_{A,V_A[X\mapsto W]}(a) \leq [\![\mu X.\psi']\!]_{C,V_C}(c) \\
\iff & \Sigma \circ [\![\psi']\!]_{A,V_A[X\mapsto W]} \leq [\![\mu X.\psi']\!]_{C,V_C} \\
\Longleftarrow & \Sigma \circ [\![\psi']\!]_{A,V_A[X\mapsto W]} \leq [\![\psi']\!]_{C,V_C[X\mapsto [\![\mu X.\psi']\!]_{C,V_C}]}
\end{array}
$$

(case $\psi = \Box\psi'$) ψ' is a $\Box L\mu$ formula. By induction hypothesis, we have $\Sigma \circ [\![\psi']\!]_{A,V_A} \leq [\![\psi']\!]_{C,V_C}$. To show $\Sigma \circ [\![\Box\psi']\!]_{A,V_A} \leq [\![\Box\psi']\!]_{C,V_C}$ is equivalent to show $\Sigma(a,c) \wedge [\![\Box\psi']\!]_{A,V_A}(a) \leq (c \rightarrow_C c') \Rightarrow [\![\psi']\!]_{C,V_C}(c')$ for every state a of A and states c, c' of C. It is proved as follows.

$$
\begin{array}{ll}
 & \Sigma(a,c) \wedge [\![\Box\psi']\!]_{A,V_A}(a) \leq (c \rightarrow_C c') \Rightarrow [\![\psi']\!]_{C,V_C}(c') \\
\iff & \Sigma(a,c) \wedge [\![\Box\psi']\!]_{A,V_A}(a) \wedge (c \rightarrow_C c') \leq [\![\psi']\!]_{C,V_C}(c') \\
\Longleftarrow & \Sigma(a',c') \wedge [\![\Box\psi']\!]_{A,V_A}(a) \wedge (a \rightarrow_A a') \leq [\![\psi']\!]_{C,V_C}(c') \\
\Longleftarrow & \Sigma(a',c') \wedge [\![\psi']\!]_{A,V_A}(a') \leq [\![\psi']\!]_{C,V_C}(c')
\end{array}
$$

(case $\psi = \varphi' \Rightarrow \psi'$) ψ' is a $\Box L\mu$ formula. By induction hypothesis, we have $\Sigma \circ [\![\psi']\!]_{A,V_A} \leq [\![\psi']\!]_{C,V_C}$. φ' is a $\Diamond L\mu$ formula. By induction hypothesis, we have $\Sigma^\circ \circ [\![\varphi']\!]_{C,V_C} \leq [\![\varphi']\!]_{A,V_A}$. To show $\Sigma \circ [\![\varphi' \Rightarrow \psi']\!]_{A,V_A} \leq [\![\varphi' \Rightarrow \psi']\!]_{C,V_C}$ is equivalent to show $\Sigma(a,c) \wedge [\![\varphi' \Rightarrow \psi']\!]_{A,V_A}(a) \leq [\![\varphi' \Rightarrow \psi']\!]_{C,V_C}(c)$ for every state a of A and every state c of C. It is proved as follows.

$$
\begin{array}{ll}
 & \Sigma(a,c) \wedge [\![\varphi' \Rightarrow \psi']\!]_{A,V_A}(a) \leq [\![\varphi' \Rightarrow \psi']\!]_{C,V_C}(c) \\
\iff & \Sigma(a,c) \wedge ([\![\varphi']\!]_{A,V_A}(a) \Rightarrow [\![\psi']\!]_{A,V_A}(a)) \leq [\![\varphi']\!]_{C,V_C}(c) \Rightarrow [\![\psi']\!]_{C,V_C}(c) \\
\iff & \Sigma(a,c) \wedge ([\![\varphi']\!]_{A,V_A}(a) \Rightarrow [\![\psi']\!]_{A,V_A}(a)) \wedge [\![\varphi']\!]_{C,V_C}(c) \leq [\![\psi']\!]_{C,V_C}(c) \\
\Longleftarrow & \Sigma(a,c) \wedge ([\![\varphi']\!]_{A,V_A}(a) \Rightarrow [\![\psi']\!]_{A,V_A}(a)) \wedge [\![\varphi']\!]_{A,V_A}(a) \leq [\![\psi']\!]_{C,V_C}(c) \\
\Longleftarrow & \Sigma(a,c) \wedge [\![\psi']\!]_{A,V_A}(a) \leq [\![\psi']\!]_{C,V_C}(c) \\
\Longleftarrow & \Sigma \circ [\![\psi']\!]_{A,V_A} \leq [\![\psi']\!]_{C,V_C}
\end{array}
$$

(case $\varphi = P$) To show $\Sigma^\circ \circ [\![P]\!]_{C,V_C} \leq [\![P]\!]_{A,V_A}$ is equivalent to show $\Sigma(a,c) \wedge \rho_C(c,P) \leq \rho_A(a,P)$ for every state a of A and every state c of C. It is implied by the condition $\rho_C \circ \Sigma \leq \rho_A$ of simulation Σ.

(case $\varphi = X$) Since $X \in \mathbf{Pos}(\psi)$, we have $\Sigma^\circ \circ V_C(X) \leq V_A(X)$. That is equivalent to $\Sigma^\circ \circ [\![X]\!]_{C,V_C} \leq [\![X]\!]_{A,V_A}$.

Other cases are also proved similarly. □

Now, Theorem 4.4 is proved as follows. Let Σ be a simulation from A to C, and V_A and V_C, respectively, be a valuation of A and C, respectively. By Lemma A.3, we have $\Sigma \circ [\![\varphi]\!]_{A,V_A} \leq [\![\varphi]\!]_{C,V_C}$. By the definition of simulations, we have $I_C \leq \Sigma \circ I_A$. Therefore, $I_A \leq [\![\varphi]\!]_{A,V_A}$ implies $I_C \leq [\![\varphi]\!]_{C,V_C}$.

様相 μ 計算のための多値モデルの模倣（in English）
(算譜科学研究速報)
発行日：2007 年 4 月 9 日
編集・発行：独立行政法人産業技術総合研究所システム検証研究センター
同連絡先：〒563-8577 大阪府池田市緑丘 1-8-31
e-mail：informatics-inquiry@m.aist.go.jp

Simulations of Multi-Valued Models for Modal μ -Calculus
(Programming Science Technical Report)
April 9, 2007
Research Center for Verification and Semantics (CVS)
National Institute of Advanced Industrial Science and Technology (AIST)
1-8-31 Midorigaoka, Ikeda, Osaka, 563-8577, Japan
e-mail: informatics- inquiry@m.aist.go.jp

AIST01-J00022-68