Algebraic Structure for a Fixed Point Logic and Abstract Interpretation

Koki Nishizawa and Makoto Takeyama

CVS, AIST and University of Tokyo CVS, AIST

Algebraic Structure for a Fixed Point Logic and Abstract Interpretation

Koki Nishizawa[12] and Makoto Takeyama[1] *

[1] Research Center of Verification and Semantics,
National Institute of Advanced Industrial Science and Technology, Japan
{koki-nishizawa, makoto.takeyama}@aist.go.jp
[2] Dept. of Computer Science, Graduate School of Information Science and Technology, University of Tokyo, Japan

Abstract. We present an algebraic structure for models of a fixed point logic. We apply this to a mathematical modelling of the notion of abstract interpretation.
The formal system of the logic has conjunction, disjunction, and restricted forms of least and greatest fixed point operators. We formulate its structure as an algebraic structure on the category **LocOrd**. An interpretation of a theory in the logic is a locally ordered functor to an algebra of the algebraic structure from a locally ordered category representing the signature, satisfying the axioms. The free algebra construction gives soundness and completeness of such interpretations.
We use the logic to express a fragment of modal μ-calculus as a theory in it, adding negated atomic propositions and modal operators in the signature. The fragment itself is expressive enough to contain the translation of CTL formulas.
Next, in order to mathematically model the notion of abstraction relations between two interpretations, we extend the algebraic structure to **Cat**-enriched one. The algebras and algebra maps remain the same, but we have as 2-cells lax transformations with left adjoints. The 2-cells represent abstraction relations. The free algebra construction now gives the soundness of the method using abstraction relations.
We also reformulate in our setting a typical construction of an abstract interpretation from a concrete one and the data for abstraction relations. We show the use of this and the above soundness in a verification of a safety problem.

1 Introduction

This paper aims to elucidate the soundness argument for abstract interpretation for a fixed point logic. Abstraction plays an important role in reducing the complexity of model checking for programs or reactive systems [13, 17, 4, 5, 3]. Central to our analysis is the notion of algebraic structure [16, 1, 8, 14] in enriched category theory [7]. We present the algebraic structure for the logic. The

* Authors acknowledge the support of a CREST project of Japan Science and Technology Corporation.

soundness of the method using abstraction relation directly follows from the free algebra construction.

We start with the variable-free presentation of our logic $R\mu$ that has a restricted form of least and greatest fixed point operations. A useful fragment of modal μ-calculus [11] can be expressed as a theory in the logic. The fragment itself is expressive enough to contain the translation of CTL formulas.

The point of our presentation of $R\mu$ is that it is an *algebraic structure*, i.e., a set of basic operations and equations among derived operations, in a categorical, generalised sense. More precisely, it is a Lawvere A-theory, **RMu**, in the sense of [14] where A = **LocOrd**, the category of locally ordered categories. The notion of Lawvere A-theory is introduced in [14] as an invariant presentation of algebraic structures corresponding to a monad on a category A (under reasonable conditions). A *model* of a Lawvere A-theory is what corresponds to an algebra of a monad. The syntactic locally ordered category given by $R\mu$ is the *free model* $F\Sigma$ of **RMu** on a given signature Σ. To give an interpretation of Σ in another model of **RMu** is equivalent to giving a map of models from $F\Sigma$ to that model, which gives a denotational semantics. When the map satisfies a theory Δ (a set of axioms), the interpretation is called a Δ-interpretation. The soundness and completeness of the class of Δ-interpretations are immediate consequences of the universality of $F\Sigma$.

In order to mathematically model the notion of abstraction relations between two Δ-interpretations, we extend our analysis in a **Cat**-enriched context. The models and maps of models remain the same, but we have as 2-cells lax transformations with left adjoints. The 2-cells represent abstraction relations. The free model construction now gives the soundness of the argument that truth of propositions in an abstract interpretation can be transfered to that in the related concrete interpretation.

We also reformulate in our setting a typical construction of an abstract interpretation from a concrete one and the data for abstraction relations.

As an example, we apply our analysis to a verification of a simple safety property.

The basic idea of this paper is similar to the paper [10]. However, there are some differences between them. First, the paper [10] gives an algebraic structure not for a logic but for a programming language. Second, an interpretation in the paper [10] is a locally ordered functor from a locally ordered category representing not the signature but the contexts. Third, arities of the algebraic structure in the paper [10] are not finitely presentable.

The paper is organised as follows. In Section 2, we define the syntax and the formal system of the logic $R\mu$. In Section 3, we define the Lawvere A-theory **RMu** for $R\mu$ and show an example of models of **RMu**. In Section 4, we define Δ-interpretations for a theory Δ. We prove soundness and completeness of the formal system for them, using the free model construction. In Section 5, we define the notion of abstraction between Δ-interpretations. In Section 6, we compare $R\mu$ with CTL and modal μ-calculus. In Section 7, we explain an example of model checking based on the abstraction.

2 Syntax and Formal System $R\mu$

In this section, we define the formal system $R\mu$ by the rules listed below. The language of $R\mu$ is parametrised by a *signature* (**Prop**, **Label**) where **Prop** is the set of basic propositions and **Label** that of labels (names for modal operators). Henceforth we fix an arbitrary signature.

There are three forms of judgements: $x\colon \textbf{sort}$ (x is a valid *$R\mu$-sort*), $\phi\colon x \to y$ (ϕ is a valid *$R\mu$-formula* from sort x to y), and $\phi \vdash \psi\colon x \to y$ (ϕ entails ψ where they are from sort x to y). The form $\phi = \psi\colon x \to y$ abbreviates the conjunction of $\psi \vdash \phi\colon x \to y$ and $\phi \vdash \psi\colon x \to y$.

A *theory* Δ in $R\mu$ is a set of entailment judgements that are treated as axioms. The judgements derivable from Δ are *Δ-theorems.*

Signature

$$\frac{}{*\colon \textbf{sort}} \qquad \frac{}{\boldsymbol{\Omega}\colon \textbf{sort}} \qquad \frac{p \in \textbf{Prop}}{p\colon * \to \boldsymbol{\Omega}} \qquad \frac{a \in \textbf{Label}}{[a]\colon \boldsymbol{\Omega} \to \boldsymbol{\Omega}}$$

Partial order

$$\frac{\phi\colon x \to y}{\phi \vdash \phi\colon x \to y} \qquad \frac{\phi \vdash \psi\colon x \to y \quad \psi \vdash \sigma\colon x \to y}{\phi \vdash \sigma\colon x \to y}$$

Composition

$$\frac{\phi\colon y \to z \quad \psi\colon x \to y}{\phi \circ \psi\colon x \to z} \qquad \frac{\phi\colon y \to z \quad \psi\colon x \to y \quad \sigma\colon w \to x}{(\phi \circ \psi) \circ \sigma = \phi \circ (\psi \circ \sigma)\colon w \to z}$$

$$\frac{\phi \vdash \sigma\colon y \to z \quad \psi \vdash \tau\colon x \to y}{\phi \circ \psi \vdash \sigma \circ \tau\colon x \to z}$$

Identity

$$\frac{x\colon \textbf{sort}}{\textbf{Id}\colon x \to x} \qquad \frac{\phi\colon x \to y}{\textbf{Id} \circ \phi = \phi\colon x \to y} \qquad \frac{\phi\colon x \to y}{\phi \circ \textbf{Id} = \phi\colon x \to y}$$

Terminal

$$\frac{}{1\colon \textbf{sort}}\,T_1 \qquad \frac{x\colon \textbf{sort}}{!_x\colon x \to 1}\,T_2 \qquad \frac{}{!_1 = \textbf{Id}\colon 1 \to 1}\,T_3 \qquad \frac{\phi\colon x \to y}{!_y \circ \phi = !_x\colon x \to 1}\,T_4$$

Binary product

$$\frac{x\colon \textbf{sort} \quad y\colon \textbf{sort}}{x \times y\colon \textbf{sort}}\,B_1 \qquad \frac{x\colon \textbf{sort} \quad y\colon \textbf{sort}}{\lambda_{x,y}\colon x \times y \to x}\,B_2 \qquad \frac{x\colon \textbf{sort} \quad y\colon \textbf{sort}}{\rho_{x,y}\colon x \times y \to y}\,B_3$$

$$\frac{\phi\colon x \to y \quad \psi\colon x \to z}{\langle \phi, \psi \rangle\colon x \to y \times z}\,B_4 \qquad \frac{x\colon \textbf{sort} \quad y\colon \textbf{sort}}{\langle \lambda_{x,y}, \rho_{x,y} \rangle = \textbf{Id}\colon x \times y \to x \times y}\,B_5$$

$$\frac{\phi\colon x \to y \quad \psi\colon x \to z}{\lambda_{y,z} \circ \langle \phi, \psi \rangle = \phi\colon x \to y}\,B_6 \qquad \frac{\phi\colon x \to y \quad \psi\colon x \to z}{\rho_{y,z} \circ \langle \phi, \psi \rangle = \psi\colon x \to z}\,B_7$$

$$\frac{\sigma\colon x \to w \quad \phi \circ \sigma = \phi'\colon x \to y \quad \psi \circ \sigma = \psi'\colon x \to z}{\langle \phi, \psi \rangle \circ \sigma = \langle \phi', \psi' \rangle\colon x \to y \times z}\ B_8$$

$$\frac{\phi \vdash \sigma\colon x \to y \quad \psi \vdash \tau\colon x \to z}{\langle \phi, \psi \rangle \vdash \langle \sigma, \tau \rangle\colon x \to y \times z}\ B_9$$

Lattice

$$\frac{x\colon \mathbf{sort}}{\bot\colon 1 \to x}\ L_1 \quad \frac{x\colon \mathbf{sort}}{\vee\colon x \times x \to x}\ L_2 \quad \frac{x\colon \mathbf{sort}}{\top\colon 1 \to x}\ L_3 \quad \frac{x\colon \mathbf{sort}}{\wedge\colon x \times x \to x}\ L_4$$

$$\frac{x\colon \mathbf{sort}}{\bot \circ !_x \vdash \mathbf{Id}\colon x \to x}\ L_5 \quad \frac{x\colon \mathbf{sort}}{\mathbf{Id} \vdash \top \circ !_x\colon x \to x}\ L_6$$

$$\frac{x\colon \mathbf{sort}}{\vee \circ \langle \mathbf{Id}, \mathbf{Id} \rangle \vdash \mathbf{Id}\colon x \to x}\ L_7 \quad \frac{x\colon \mathbf{sort}}{\mathbf{Id} \vdash \langle \mathbf{Id}, \mathbf{Id} \rangle \circ \vee\colon x \times x \to x \times x}\ L_8$$

$$\frac{x\colon \mathbf{sort}}{\mathbf{Id} \vdash \wedge \circ \langle \mathbf{Id}, \mathbf{Id} \rangle\colon x \to x}\ L_9 \quad \frac{x\colon \mathbf{sort}}{\langle \mathbf{Id}, \mathbf{Id} \rangle \circ \wedge \vdash \mathbf{Id}\colon x \times x \to x \times x}\ L_{10}$$

Least fixed point of restricted formula: $\mu(\phi, \psi)$ is the least fixed point of F where $F\sigma \triangleq \vee \circ \langle \phi, \psi \circ \sigma \rangle$.

$$\frac{\phi\colon x \to y \quad \psi\colon y \to y}{\mu(\phi, \psi)\colon x \to y}\ M_1 \quad \frac{\phi\colon x \to y \quad \psi\colon y \to y}{\phi \vdash \mu(\phi, \psi)\colon x \to y}\ M_2$$

$$\frac{\phi\colon x \to y \quad \psi\colon y \to y}{\psi \circ \mu(\phi, \psi) \vdash \mu(\phi, \psi)\colon x \to y}\ M_3 \quad \frac{\phi \vdash \sigma\colon x \to y \quad \psi \circ \sigma \vdash \sigma\colon x \to y}{\mu(\phi, \psi) \vdash \sigma\colon x \to y}\ M_4$$

$$\frac{\sigma\colon x \to y \quad \phi\colon y \to z \quad \psi\colon z \to z}{\mu(\phi, \psi) \circ \sigma = \mu(\phi \circ \sigma, \psi)\colon x \to z}\ M_5$$

Greatest fixed point of restricted formula: $\nu(\phi, \psi)$ is the greatest fixed point of F where $F\sigma \triangleq \wedge \circ \langle \phi, \psi \circ \sigma \rangle$.

$$\frac{\phi\colon x \to y \quad \psi\colon y \to y}{\nu(\phi, \psi)\colon x \to y}\ N_1 \quad \frac{\phi\colon x \to y \quad \psi\colon y \to y}{\nu(\phi, \psi) \vdash \phi\colon x \to y}\ N_2$$

$$\frac{\phi\colon x \to y \quad \psi\colon y \to y}{\nu(\phi, \psi) \vdash \psi \circ \nu(\phi, \psi)\colon x \to y}\ N_3 \quad \frac{\sigma \vdash \phi\colon x \to y \quad \sigma \vdash \psi \circ \sigma\colon x \to y}{\sigma \vdash \nu(\phi, \psi)\colon x \to y}\ N_4$$

$$\frac{\sigma\colon x \to y \quad \phi\colon y \to z \quad \psi\colon z \to z}{\nu(\phi, \psi) \circ \sigma = \nu(\phi \circ \sigma, \psi)\colon x \to z}\ N_5$$

Δ-Axioms

$$\frac{}{\phi \vdash \psi\colon x \to y}\ \text{(provided it is in } \mathit{\Delta}\text{)}$$

3 The Algebraic Structure for Semantics of $R\mu$

In this section, we give the algebraic structure **RMu** for the logic $R\mu$. The algebraic semantics of $R\mu$ in the next section is based on this structure.

We present **RMu** as Lawvere A-theory [14]. The notion of Lawvere A-theory generalises that of classical Lawvere theory [1] in two points. First, we can enrich our theories in a category V that is locally finitely presentable as a symmetric monoidal closed category. Second, we can give arities of our theories by finitely presentable objects of a locally finitely presentable V-category A. The classical Lawvere theories are the instances where $V = A = \mathbf{Set}$.

We write A_f for a skeleton of the full sub-V-category of A given by the finitely presentable objects of A, and we let $\iota\colon\ A_f \to A$ denote the inclusion V-functor. Following the canonical reference for enriched categories [7], we denote the composite V-functor

$$A \xrightarrow{Y} [A^{\mathrm{op}}, V] \xrightarrow{[\iota^{\mathrm{op}}, V]} [A_f^{\mathrm{op}}, V]$$

by $\tilde{\iota}$, where Y is an enriched version of the Yoneda embedding.

Definition 1 (Lawvere A-theory). *A* Lawvere A-theory *is a small V-category L together with an identity-on-objects strict finite V-limit preserving V-functor $J\colon\ A_f^{\mathrm{op}} \to L$.*

The objects of L are exactly the objects of A_f^{op}; they are to be understood as generalised *arities*. The arrows of L are *operations*. (In the classical case, an arity is a finite set $n = 0, 1, \cdots, n-1$, and $f : m \to n$ is an operation taking m arguments and returning n results.)

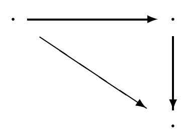
The formal system $R\mu$ has sorts, formulas between sorts, and inequalities between formulas. To give semantics for them naturally, we consider locally ordered categories with certain structure.

Definition 2. **LocOrd** *is the category (i.e.,* **Set***-category) of locally ordered small categories and locally ordered functors.*

We can prove that this is a locally finitely presentable category.

For later use, we name some finitely presentable objects in **LocOrd**.

- 0 : the empty locally ordered category (no objects, no arrows).
- 1 : one object and the identity arrow.
- $\mathbf{2} = \{\mathbf{a} \xrightarrow{\mathbf{s}} \mathbf{b}\}$: two objects $\mathbf{a}$, $\mathbf{b}$ and one non-identity arrow $\mathbf{s}$.
- $\mathbf{A_3}$: two objects and two parallel arrows subject to an inequality between the arrows.
- $\mathbf{3}$: three objects and three non-identity arrows arranged as in the triangle below, which commutes.



– $\mathbf{A_7}$: two objects $\mathbf{x}$, $\mathbf{y}$ and non-identity arrows generated from $\mathbf{p}\colon \mathbf{x} \to \mathbf{y}$ and $\mathbf{f}\colon \mathbf{y} \to \mathbf{y}$.

We define Lawvere **LocOrd**-theory **RMu** corresponding to the formal system $R\mu$. We give **RMu** as the locally ordered category freely generated from $(\mathbf{LocOrd})_f^{\mathrm{op}}$ by adding certain operations, subject to the condition that certain diagrams commute and that the inclusion is strictly finite-limit preserving. For each rule of $R\mu$, we introduce one operation and a few diagrams. Since this procedure follows the same pattern for all rules, we show only some examples. The complete definition of **RMu** is in Appendix A.

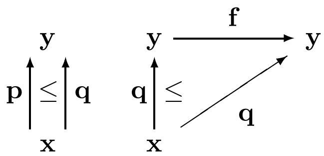
For example, we consider the four rules $T_1 - T_4$ for terminal objects. These are specified by four operations corresponding to them and seven diagrams in Appendix A. The shapes of the premise and the consequence parts of a rule determine the domain and codomain arities (which are locally ordered categories) of the corresponding rule. Here we consider that an object and an arrow correspond to a sort and a formula, respectively. Thus, the four operations have the following arities.

$$\begin{aligned} T_1 &\colon\ 0 \to 1 \\ T_2 &\colon\ 1 \to \mathbf{2} \\ T_3 &\colon\ 0 \to \mathbf{2} \\ T_4 &\colon\ \mathbf{2} \to \mathbf{3} \end{aligned}$$

Next, we consider the rule M_4 for the least fixed points.

$$\frac{\phi \vdash \sigma\colon\ x \to y \quad \psi \circ \sigma \vdash \sigma\colon\ x \to y}{\mu(\phi, \psi) \vdash \sigma\colon\ x \to y}\ M_4$$

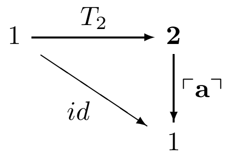
In making this rule an operation, it is crucial that we can specify a locally ordered category as an arity. Here we consider that $(-) \vdash (-)$ corresponds to an inequality among arrows. So the shape of the premise is the locally ordered category $\mathbf{A_9}$ with objects $\mathbf{x}$, $\mathbf{y}$ and arrows generated from $\mathbf{p}, \mathbf{q}\colon\ \mathbf{x} \to \mathbf{y}$ and $\mathbf{f}\colon\ \mathbf{y} \to \mathbf{y}$ subject to inequalities $\mathbf{p} \leq \mathbf{q}$ and $\mathbf{f} \circ \mathbf{q} \leq \mathbf{q}$.



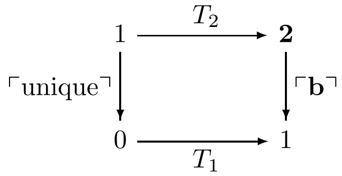
The arity of the corresponding operation is $M_4\colon\ \mathbf{A_9} \to \mathbf{A_3}$.

We similarly introduce thirty-three operations for all rules, except for the rules about identity, composition, partial order (since they are built-in in the setting), signature, and Δ-axioms (to be treated later).

Next, we introduce diagrams for the rules of $R\mu$. Two kinds of diagrams are necessary for each rule. The first kind specifies that part of the codomain arity which should directly come from the domain arity: For example, in the rule T_2 the sort x in the the premise part appears in the consequence. To express that the two occurrences are equal, we introduce the diagram below. Here, $\ulcorner \mathbf{a} \urcorner$ is the functor from 1 to $\mathbf{2} = \{\mathbf{a} \xrightarrow{\mathbf{s}} \mathbf{b}\}$ naming $\mathbf{a}$. In $(\mathbf{LocOrd})_f^{\mathrm{op}}$, the direction of the arrow becomes $\ulcorner\mathbf{a}\urcorner\colon\ \mathbf{2} \to 1$.

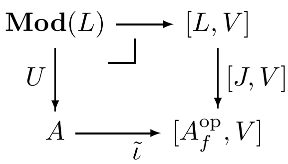


The second kind of diagrams give constraints that certain part of the codomain arity must be given by some other operation. For example, $\mathbf{b}$ in the codomain arity $\mathbf{2}$ of T_2 must be given by T_1. Therefore, we introduce the following diagram where $\ulcorner$unique$\urcorner$ and $\ulcorner\mathbf{b}\urcorner$ are the obvious functors.



Other diagrams in the definition of **RMu** in Appendix A are similarly obtained.

Definition 3 (Model of Lawvere A-theory). *For a Lawvere A-theory L with $J\colon\ A_f^{\mathrm{op}} \to L$, a* model *is an object of* $\mathbf{Mod}(L)$ *given by the following pullback in the category V-***Cat** *of locally small V-categories.*



So, a model of Lawvere A-theory (L, J) is a pair of an object $a \in A$ and a V-functor $S\colon\ L \to V$ such that $A(\iota -, a) = S \circ J\colon\ A_f^{\mathrm{op}} \to V$. To see what this means, consider a model (C, S) of **RMu** where $C \in \mathbf{LocOrd}$ and $S\colon\ \mathbf{RMu} \to \mathbf{Set}$. S sends the operation $M_1\colon\ \mathbf{A_7} \to \mathbf{2}$, which corresponds to the rule M_1, to a function $SM_1\colon\ \mathbf{LocOrd}(\mathbf{A_7}, C) \to \mathbf{LocOrd}(\mathbf{2}, C)$. For $G \in \mathbf{LocOrd}(\mathbf{A_7}, C)$, the diagrams relevant to M_1 requires that $(SM_1)G$ must have the following:

- $G\mathbf{x} = ((SM_1)G)\mathbf{a}$ and $G\mathbf{y} = ((SM_1)G)\mathbf{b}$
- $G\mathbf{p} \le ((SM_1)G)\mathbf{s}$ and $G\mathbf{f} \circ ((SM_1)G)\mathbf{s} \le ((SM_1)G)\mathbf{s}$
- If $k\colon\ G\mathbf{x} \to G\mathbf{y}$ satisfies $G\mathbf{p} \le k$ and $G\mathbf{f} \circ k \le k$, then $((SM_1)G)\mathbf{s} \le k$.

Example 1. The following data $\mathbf{Pos_{CL}} = (C, S)$ gives a model of Lawvere **LocOrd**-theory **RMu**.

- Objects of C are complete lattices[3].

[3] In order to fit C in **LocOrd**, we should limit the size of lattices, or consider **LocOrd** in a higher universe of sets. Either way is not a problem, but here we generally wave our hands on the size issue.

– Arrows of C are all monotone functions.
– Orders are given by element-wise orders.
– The structure for 1 is given by the single-element complete lattice.
– The structure for $\times$ is given by the binary product of two complete lattices.
– Structures for $\bot$, $\top$, $\vee$, and $\wedge$ are given by least element, greatest element, join, and meet of complete lattices, respectively.
– SM_1 sends G to $(SM_1)G$ such that $((SM_1)G)\mathbf{s} = \cap\{r \mid G\mathbf{p} \cup (G\mathbf{f} \circ r) \leq r\}$.
– SN_1 sends G to $(SN_1)G$ such that $((SN_1)G)\mathbf{s} = \cup\{r \mid r \leq G\mathbf{p} \cap (G\mathbf{f} \circ r)\}$.

4 Algebraic Semantics of $R\mu$

In this section, we give the notion of Δ-interpretations using the free model of Lawvere **LocOrd**-theory **RMu**. It is easy to prove soundness and completeness of the formal system $R\mu$ with respect to the class of Δ-interpretations.

We regard signature $(\mathbf{Prop}, \mathbf{Label})$ as the locally ordered category $\Sigma = \Sigma(\mathbf{Prop}, \mathbf{Label})$ generated from objects $*$, $\mathbf{\Omega}$, an arrow $p\colon * \to \mathbf{\Omega}$ for each $p \in \mathbf{Prop}$, and an arrow $[a]\colon \mathbf{\Omega} \to \mathbf{\Omega}$ for each $a \in \mathbf{Label}$. The syntactic entities of $R\mu$ can be organised into the locally ordered category C defined by

– objects: $R\mu$-sorts
– arrows: $R\mu$-formulas quotiented by
– inequality: $\emptyset$-theorem (i.e., Δ-theorem for $\Delta = \emptyset$)

Then, we can easily define $S\colon \mathbf{RMu} \to \mathbf{Set}$ such that (C, S) is a model in $\mathbf{Mod}(\mathbf{RMu})$. We write $F\Sigma$ for (C, S) and $\eta\colon\ \Sigma \to UF\Sigma$ for the trivial inclusion.

Theorem 1 (Free model). *For each model M of Lawvere* **LocOrd***-theory* **RMu***, any $m \in \mathbf{LocOrd}(\Sigma, UM)$ is equal to $U\bar{m}\circ\eta$ for a unique $\bar{m} \in \mathbf{Mod}(\mathbf{RMu})(F\Sigma, M)$.*

Proof. The rules for sort- and formula- judgements of $R\mu$ are syntax-directed, i.e., judgements of the form $x\colon$ **sort** or $\phi\colon\ x \to y$ have at most one derivation. Definition of $U\bar{m}$ is given by induction on the structure of this derivation.

We write $[\![-]\!]_m$ for $U\bar{m}$ to emphasise that it is a semantics function sending $R\mu$-sorts and formulas to semantic values in the model M.

Example 2 (Kripke semantics). A Kripke structure $(S,\ R \subseteq S{\times}\mathbf{Label}{\times}S,\ Q\colon\ S \to \wp(\mathbf{Prop}))$ gives rise to the interpretation $m \in \mathbf{LocOrd}(\Sigma, U\mathbf{Pos_{CL}})$ given by

$m* = \{\cdot\}$ (single-element complete lattice)
$m\mathbf{\Omega} = \wp(S)$
$mp\colon\ \cdot \mapsto \{s \in S \mid p \in Q(s)\}$ for any $p \in \mathbf{Prop}$
$m[a]\colon\ X \mapsto \{s \in S \mid \forall s' \in S.(s, a, s') \in R \Rightarrow s' \in X\}$ for any $a \in \mathbf{Label}$

Definition 4 (Δ-interpretation). *For $M \in \mathbf{Mod}(\mathbf{RMu})$ and a theory Δ, an arrow $m \in \mathbf{LocOrd}(\Sigma, UM)$ is a* Δ-interpretation *if $[\![\phi]\!]_m \leq [\![\psi]\!]_m$ for each axiom $\phi \vdash \psi : x \to y$ in Δ.*

Theorem 2 (Soundness). *A Δ-interpretation $m \in \mathbf{LocOrd}(\Sigma, UM)$ satisfies $[\![\phi]\!]_m \leq [\![\psi]\!]_m$ for any Δ-theorem $\phi \vdash \psi \colon x \to y$.*

Proof. The soundness of the rules for partial order, composition, and identity is obvious. That of other rules can be verified through analysis similar to the one preceding Example 1.

We prove completeness by the construction of a generic model [15], which is a quotient of $F\Sigma$ by Δ.

Theorem 3 (Completeness). *For $R\mu$-formulas $\phi\colon x \to y$ and $\psi\colon x \to y$, the judgement $\phi \vdash \psi\colon x \to y$ is a Δ-theorem if any Δ-interpretation m satisfies $[\![\phi]\!]_m \leq [\![\psi]\!]_m$.*

Proof. Similarly to $F\Sigma$, we give a locally ordered category $F\Sigma/\Delta$:

- objects: $R\mu$-sorts
- arrows: $R\mu$-formulas quotiented by
- inequality: Δ-theorems

This time, the trivial embedding $\eta_\Delta : \Sigma \to F\Sigma/\Delta$ becomes a Δ-interpretation. More over, we have that $\phi \vdash \psi\colon x \to y$ is a Δ-theorem whenever $[\![\phi]\!]_{\eta_\Delta} \leq [\![\psi]\!]_{\eta_\Delta}$ (cf. Section 5.7 of [15]).

The existence of the free or generic models is automatic for any Lawvere A-theory, but we gave the explicit description for the proof of completeness in this sense.

5 Abstraction between Interpretations

In this section, we give the notion of abstraction from a Δ-interpretation to another with the same codomain.

We use enriched category theory [7] to uniformly extend the analysis of the previous sections, enriching the set of interpretations $\mathbf{LocOrd}(\Sigma, UM)$ to a category having abstractions as arrows. Following [9], we model abstractions as certain lax transformations.

Definition 5. $\mathbf{LocOrd}_{lr}$ *is the 2-category (i.e.,* **Cat***-category) given by*

- *objects: locally ordered small categories*
- *arrows: locally ordered functors*
- *2-cells: lax transformations whose components have left adjoints (i.e., lax transformation $\gamma\colon m \to n$ such that each component $\gamma_x\colon mx \to nx$ has a left adjoint; namely, there exists an $\alpha_x\colon nx \to mx$ such that $\alpha_x \circ \gamma_x \leq id_{mx}$ and $id_{nx} \leq \gamma_x \circ \alpha_x$.)*

Similarly to the paper [9], we can prove that it is a locally finitely presentable 2-category.

Next, we extend the **Set**-enriched Lawvere **LocOrd**-theory **RMu** to the **Cat**-enriched Lawvere $\mathbf{LocOrd}_{lr}$-theory **ERMu**.

Definition 6. *Lawvere* $\mathbf{LocOrd}_{lr}$*-theory* $\mathbf{ERMu}$ *is the 2-category freely generated from* $(\mathbf{LocOrd}_{lr})_f^{\mathrm{op}}$ *by adding the same operations and diagrams for* $\mathbf{RMu}$ *in Appendix A.*

Theorem 4. *There exists a bijection between the class of all models for* $\mathbf{ERMu}$ *and the class of all models for* $\mathbf{RMu}$.

Proof. Let $\mathbf{ob}\colon \mathbf{Cat} \to \mathbf{Set}$ be the functor that sends a category to the set of the objects. If $(C, S\colon \mathbf{ERMu} \to \mathbf{Cat})$ is a model of $\mathbf{ERMu}$, then $(C, \mathbf{ob} \circ S\colon \mathbf{RMu} \to \mathbf{Set})$ is a model of $\mathbf{RMu}$.

Conversely, given a model $(C, S\colon \mathbf{RMu} \to \mathbf{Set})$ of $\mathbf{RMu}$, there exists a unique model $(C, T\colon \mathbf{ERMu} \to \mathbf{Cat})$ of $\mathbf{ERMu}$ such that $\mathbf{ob} \circ T = S$. Here we show that, for the operation M_1, $TM_1\colon \mathbf{LocOrd}_{lr}(\mathbf{A_7}, C) \to \mathbf{LocOrd}_{lr}(\mathbf{2}, C)$ is uniquely determined.

Let $\gamma\colon G \to G' \in \mathbf{LocOrd}_{lr}(\mathbf{A_7}, C)$. Writing out its lax naturality, we have

$$\begin{array}{ccc} G\mathbf{x} & \xrightarrow{G\mathbf{p}} & G\mathbf{y} \\ \downarrow{\scriptstyle \gamma_{\mathbf{x}}} & \leq & \downarrow{\scriptstyle \gamma_{\mathbf{y}}} \\ G'\mathbf{x} & \xrightarrow[G'\mathbf{p}]{} & G'\mathbf{y} \end{array} \qquad \begin{array}{ccc} G\mathbf{y} & \xrightarrow{G\mathbf{f}} & G\mathbf{y} \\ \downarrow{\scriptstyle \gamma_{\mathbf{y}}} & \leq & \downarrow{\scriptstyle \gamma_{\mathbf{y}}} \\ G'\mathbf{y} & \xrightarrow[G'\mathbf{f}]{} & G'\mathbf{y} \end{array}$$

We need to define $(TM_1)\gamma$ that is lax natural, i.e.,

$$\begin{array}{ccc} ((TM_1)G)\mathbf{a} & \xrightarrow{((TM_1)G)\mathbf{s}} & ((TM_1)G)\mathbf{b} \\ {\scriptstyle ((TM_1)\gamma)_{\mathbf{a}}}\downarrow & \leq & \downarrow{\scriptstyle ((TM_1)\gamma)_{\mathbf{b}}} \\ ((TM_1)G')\mathbf{a} & \xrightarrow[((TM_1)G')\mathbf{s}]{} & ((TM_1)G')\mathbf{b} \end{array}$$

The object part of TM_1 must be that of SM_1, so $((TM_1)G)\mathbf{s} = ((SM_1)G)\mathbf{s}$ and $((TM_1)G')\mathbf{s} = ((SM_1)G')\mathbf{s}$. In the $\mathbf{Cat}$ enrichment, the diagram for M_1 such as $\ulcorner \mathbf{a}, \mathbf{b} \urcorner \circ M_1 = \ulcorner \mathbf{x}, \mathbf{y} \urcorner$ represent not only equations for the object part, but also ones for the arrow part. So we must define not only that $((TM_1)G)\mathbf{a} = G\mathbf{x}$ and $((TM_1)G')\mathbf{a} = G'\mathbf{x}$ but also that $((TM_1)\gamma)_{\mathbf{a}} = \gamma_{\mathbf{x}}$; similarly, $((TM_1)\gamma)_{\mathbf{b}} = \gamma_{\mathbf{y}}$.

It remains to verify that $(TM_1)\gamma$ thus defined is lax natural, that is:

$$\begin{array}{ccc} G\mathbf{x} & \xrightarrow{((SM_1)G)\mathbf{s}} & G\mathbf{y} \\ \downarrow{\scriptstyle \gamma_{\mathbf{x}}} & \leq & \downarrow{\scriptstyle \gamma_{\mathbf{y}}} \\ G'\mathbf{x} & \xrightarrow[((SM_1)G')\mathbf{s}]{} & G'\mathbf{y} \end{array}$$

This is equivalent to $((SM_1)G')\mathbf{s} \leq \gamma_{\mathbf{y}} \circ ((SM_1)G)\mathbf{s} \circ \alpha_{\mathbf{x}}$ where $\alpha_{\mathbf{x}}$ is the left adjoint to $\gamma_{\mathbf{x}}$. So we are done by the operation for M_4 if $G'\mathbf{p} \leq$ (RHS) and $G'\mathbf{f} \circ$ (RHS) $\leq$ (RHS). Indeed, we have that

$$\begin{aligned} G'\mathbf{p} &\leq G'\mathbf{p} \circ \gamma_{\mathbf{x}} \circ \alpha_{\mathbf{x}} && \text{(by adjointness)} \\ &\leq \gamma_{\mathbf{y}} \circ G\mathbf{p} \circ \alpha_{\mathbf{x}} && \text{(by lax naturality with respect to } \mathbf{p}\text{)} \\ &\leq \gamma_{\mathbf{y}} \circ ((SM_1)G)\mathbf{s} \circ \alpha_{\mathbf{x}} && \text{(by the operation for } M_2\text{)} \end{aligned}$$

and that

$$\begin{aligned} & G'\mathbf{f} \circ \gamma_{\mathbf{y}} \circ ((SM_1)G)\mathbf{s} \circ \alpha_{\mathbf{x}} \\ & \quad \leq \gamma_{\mathbf{y}} \circ G\mathbf{f} \circ ((SM_1)G)\mathbf{s} \circ \alpha_{\mathbf{x}} && \text{(by lax naturality with respect to } \mathbf{f}) \\ & \quad \leq \gamma_{\mathbf{y}} \circ ((SM_1)G)\mathbf{s} \circ \alpha_{\mathbf{x}} && \text{(by the operation for } M_3) \end{aligned}$$

Theorem 5 (Free model). *There exists an isomorphism between the category* $\mathbf{LocOrd}_{lr}(\Sigma, UM)$ *and the category* $\mathbf{Mod}(\mathbf{ERMu})(F\Sigma, M)$.

Proof. The bijection on the object classes are given by Theorem 1 together with Theorem 4. The arrow part is proved similarly to the latter.

Let $\bar{\gamma}\colon \bar{m} \to \bar{n}$ be the arrow in $\mathbf{Mod}(\mathbf{ERMu})(F\Sigma, M)$ that corresponds to an arrow $\gamma\colon m \to n$ in $\mathbf{LocOrd}_{lr}(\Sigma, UM)$ by the above theorem. This correspondence implies a property expected for the notion of abstraction defined below.

Definition 7 (Abstraction). *An* abstraction γ *from a* Δ*-interpretation* m *to another* n *is a 2-cell* $\gamma\colon m \to n$.

Corollary 1 (Soundness for abstraction). *For any abstraction* $\gamma\colon m \to n$ *and any* $R\mu$*-formula* $\phi\colon x \to y$, $[\![\phi]\!]_n \circ \bar{\gamma}_x \leq \bar{\gamma}_y \circ [\![\phi]\!]_m$.

Example 3 (Simulation). An abstraction for Kripke models (Example 2) is known as simulation [13, 17]. Combined with the translation in Section 6, the above corollary implies a part of the theorem that a simulation preserves certain formulas in modal μ-calculus [12, 17].

The next theorem gives a construction of an abstract $\emptyset$-interpretation (i.e., $\Delta = \emptyset$) from a concrete interpretation. This is a generalisation of the typical construction when model checking a program using data abstraction [4, 5, 3].

Theorem 6 (Construction of abstract interpretation). *Let* M *be a model of Lawvere* $\mathbf{LocOrd}$*-theory* $\mathbf{RMu}$ *and* $m \in \mathbf{LocOrd}_{lr}(\Sigma, UM)$. *For any objects* $n*, n\mathbf{\Omega} \in UM$ *and right adjoint arrows* $\gamma_* \in UM(m*, n*)$, $\gamma_{\mathbf{\Omega}} \in UM(m\mathbf{\Omega}, n\mathbf{\Omega})$, *the data* $(n*, n\mathbf{\Omega})$ *extends to an interpretation* $n \in \mathbf{LocOrd}_{lr}(\Sigma, UM)$ *that makes* $(\gamma_*, \gamma_{\mathbf{\Omega}})$ *an abstraction* $\gamma : m \to n$.

Proof. With left adjoints $\alpha_* \dashv \gamma_*$ and $\alpha_{\mathbf{\Omega}} \dashv \gamma_{\mathbf{\Omega}}$, the arrow part of n is given by

$$\begin{aligned} np &= \gamma_* \circ mp \circ \alpha_* && \text{(for any } p \in \mathbf{Prop}) \\ n[a] &= \gamma_{\mathbf{\Omega}} \circ m[a] \circ \alpha_{\mathbf{\Omega}} && \text{(for any } a \in \mathbf{Label}) \end{aligned}$$

The two adjointness make γ lax natural.

6 Comparison with Modal μ-Calculus

In this section, we compare our logic $R\mu$ with modal μ-calculus $L\mu$ [11] and CTL [2]. First, we introduce syntactic restriction $L\mu^-$ of $L\mu$. Next, we prove that $L\mu^-$ can be translated in $R\mu$ and that CTL can be translated in $L\mu^-$.

Definition 8. $L\mu^-$-formulas *are given by the grammar*

$$\begin{array}{rl}\varphi ::= & \bot \mid \top \mid \varphi \vee \varphi \mid \varphi \wedge \varphi \mid \mu Z.(\varphi \vee \varphi) \mid \nu Z.(\varphi \wedge \varphi) \\ \mid & p \mid \neg p \mid \Diamond\varphi \mid \Box\varphi \mid Z\end{array}$$

where

- *p is a propositional constant taken from a given set $\mathbf{Prop}_{L\mu^-}$ of such constants.*
- *Z is a propositional variable.*
- *$\mu Z.(\varphi_1 \vee \varphi_2)$ and $\nu Z.(\varphi_1 \wedge \varphi_2)$ must satisfy that $Z \notin FV(\varphi_1)$ and that $FV(\varphi_2) \subseteq \{Z\}$. (We write $FV(\varphi)$ for the set of free variables in φ.)*

For $L\mu^-$-formulas φ and ψ, the result $\psi[\varphi/Z]$ of capture-avoiding substitution of φ for Z in ψ is a $L\mu^-$-formula. The Kripke semantics of $L\mu^-$ is the same as that for $L\mu$; we write $K, s \models_{L\mu^-} \varphi$ when a state s satisfies φ in a Kripke structure K. Also, the inference rules of $L\mu^-$ are the instances of those of $L\mu$ in which only $L\mu^-$-formulas appear; we write $\varphi \leqslant_{L\mu^-} \psi$ for inequalities derivable in $L\mu^-$.

Our translation of $L\mu^-$-formulas assumes the following signature for $R\mu$.

$$\begin{array}{r}\mathbf{Prop} = \mathbf{Prop}_{L\mu^-} \cup \{\neg p \mid p \in \mathbf{Prop}_{L\mu^-}\} \\ \mathbf{Label} = \{\Box, \Diamond\}\end{array}$$

The meaning of the constants is specified by the theory $\Delta_{L\mu^-}$, which consists of the axioms for positive modal algebras [6] and negated basic propositions.

$$\begin{array}{l}\wedge \circ (\mathbf{Id} \times \vee) = \vee \circ \langle \wedge \circ (\mathbf{Id} \times \lambda), \wedge \circ (\mathbf{Id} \times \rho)\rangle \colon\ \mathbf{\Omega} \times (\mathbf{\Omega} \times \mathbf{\Omega}) \to \mathbf{\Omega} \\ \wedge \circ ([\Diamond] \times [\Box]) \vdash [\Diamond] \circ \wedge \colon\ \mathbf{\Omega} \times \mathbf{\Omega} \to \mathbf{\Omega} \\ [\Box] \circ \vee \vdash \vee \circ ([\Diamond] \times [\Box]) \colon\ \mathbf{\Omega} \times \mathbf{\Omega} \to \mathbf{\Omega} \\ [\Diamond] \circ \bot = \bot \colon\ 1 \to \mathbf{\Omega} \\ [\Diamond] \circ \vee = \vee \circ ([\Diamond] \times [\Diamond]) \colon\ \mathbf{\Omega} \times \mathbf{\Omega} \to \mathbf{\Omega} \\ [\Box] \circ \top = \top \colon\ 1 \to \mathbf{\Omega} \\ [\Box] \circ \wedge = \wedge \circ ([\Box] \times [\Box]) \colon\ \mathbf{\Omega} \times \mathbf{\Omega} \to \mathbf{\Omega} \\ \wedge \circ \langle p, \neg p\rangle \circ \top = \bot \colon\ 1 \to \mathbf{\Omega} \quad (p \in \mathbf{Prop}_{L\mu^-}) \\ \vee \circ \langle p, \neg p\rangle \circ \top = \top \colon\ 1 \to \mathbf{\Omega} \quad (p \in \mathbf{Prop}_{L\mu^-})\end{array}$$

Definition 9 ($L\mu^-$-formula to $R\mu$-formula). *Let Γ be a set of propositional variables, $\mathbf{\Omega}^\Gamma$ the product sort of Γ copies of $\mathbf{\Omega}$, and $\pi_{Z,\Gamma}$ the projection corresponding to $Z \in \Gamma$ (i.e., $\pi_{Z,\Gamma}$ consists of λ's and ρ's). For any $L\mu^-$-formula φ such that $FV(\varphi) \subseteq \Gamma$, $R\mu$-formula $|\varphi|_\Gamma \colon \mathbf{\Omega}^\Gamma \to \mathbf{\Omega}$ is given by the following*

$$\begin{array}{rlrl}|\bot|_\Gamma &= \bot \circ !_{\mathbf{\Omega}^\Gamma} & |p|_\Gamma &= p \circ \top \circ !_{\mathbf{\Omega}^\Gamma} \\ |\top|_\Gamma &= \top \circ !_{\mathbf{\Omega}^\Gamma} & |\neg p|_\Gamma &= \neg p \circ \top \circ !_{\mathbf{\Omega}^\Gamma} \\ |\varphi \vee \psi|_\Gamma &= \vee \circ \langle |\varphi|_\Gamma, |\psi|_\Gamma \rangle & |\Diamond\varphi|_\Gamma &= [\Diamond] \circ |\varphi|_\Gamma \\ |\varphi \wedge \psi|_\Gamma &= \wedge \circ \langle |\varphi|_\Gamma, |\psi|_\Gamma \rangle & |\Box\varphi|_\Gamma &= [\Box] \circ |\varphi|_\Gamma \\ |\mu Z.(\varphi \vee \psi)|_\Gamma &= \mu(|\varphi|_\Gamma, |\psi|_{\{Z\}}) & |Z|_\Gamma &= \pi_{Z,\Gamma} \\ |\nu Z.(\varphi \wedge \psi)|_\Gamma &= \nu(|\varphi|_\Gamma, |\psi|_{\{Z\}}) & & \end{array}$$

Lemma 1. *If* $FV(\varphi) \subseteq \Gamma$*,* $Z \notin FV(\varphi)$*, and* $FV(\psi) \subseteq \{Z\}$*, then* $|\psi[\varphi/Z]|_\Gamma = |\psi|_{\{Z\}} \circ |\varphi|_\Gamma$.

Proof. By induction on the structure of ψ.

The translation is faithful with respect to the Kripke semantics in the following sense. Given a Kripke structure $K = (S,\, R \subseteq S \times S,\, Q\colon\; S \to \wp(\mathbf{Prop}_{L\mu^-}))$, define the interpretation $m_K \in \mathbf{LocOrd}(\Sigma, U\mathbf{Pos_{CL}})$ by

$$
\begin{array}{ll}
m_K * = \{\cdot\} & \text{(single-element complete lattice)} \\
m_K \mathbf{\Omega} = \wp(S) & \\
m_K\ \ p\colon\; \cdot \mapsto \{s \in S \mid p \in Q(s)\} & (p \in \mathbf{Prop}_{L\mu^-}) \\
m_K \neg p\colon\; \cdot \mapsto \{s \in S \mid p \notin Q(s)\} & (p \in \mathbf{Prop}_{L\mu^-}) \\
m_K[\Diamond]\colon\; X \mapsto \{s \in S \mid \exists s' \in X.(s,s') \in R\} & \\
m_K[\Box]\colon\; X \mapsto \{s \in S \mid \forall s' \in S.(s,s') \in R \Rightarrow s' \in X\} &
\end{array}
$$

Theorem 7. *The interpretation* m_K *is a* $\Delta_{L\mu^-}$*-interpretation. Moreover, for any closed* $L\mu^-$*-formula* φ *and* ψ*,*

$$\forall s.(K, s \models_{L\mu^-} \varphi \Rightarrow K, s \models_{L\mu^-} \psi) \Longleftrightarrow [\![|\varphi|_\emptyset]\!]_{m_K} \leq [\![|\psi|_\emptyset]\!]_{m_K}$$

Proof. Lemma 1 and induction on φ show that $[\![|\varphi|_\emptyset]\!]_{m_K} = \{s \mid K, s \models_{L\mu^-} \varphi\}$.

Theorem 8. *For any* $L\mu^-$*-formulas* φ *and* ψ *with* $FV(\varphi,\psi) \subseteq \Gamma$*,*

$$\varphi \leqslant_{L\mu^-} \psi \Longleftrightarrow |\varphi|_\Gamma \vdash |\psi|_\Gamma\colon\; \mathbf{\Omega}^\Gamma \to \mathbf{\Omega} \text{ is a } \Delta_{L\mu^-}\text{−theorem}$$

Proof. By induction on the derivations in $L\mu^-$ and in $R\mu$.

Next, we compare CTL-formula with $L\mu^-$-formula. Semantics of CTL is given by Kripke structures with total transition relations. The translation $||-||$ from CTL-formulas in the negation normal form to closed modal μ-formula is well-known [2]. It is direct to check that $||\varphi||$ is a $L\mu^-$-formula for any negation normal CTL-formula φ.

$$
\begin{aligned}
||p|| &= p \\
||\neg p|| &= \neg p \\
||\mathbf{EX}\varphi|| &= \Diamond||\varphi|| \\
||\mathbf{AX}\varphi|| &= \Box||\varphi|| \\
||\mathbf{EF}\varphi|| &= \mu Z.(||\varphi|| \vee \Diamond Z) \\
||\mathbf{AF}\varphi|| &= \mu Z.(||\varphi|| \vee \Box Z) \\
||\mathbf{E}(\varphi\mathbf{U}\psi)|| &= \mu Z.(||\psi|| \vee (||\varphi|| \wedge \Diamond Z)) \\
||\mathbf{A}(\varphi\mathbf{U}\psi)|| &= \mu Z.(||\psi|| \vee (||\varphi|| \wedge \Box Z)) \\
||\mathbf{EG}\varphi|| &= \nu Z.(||\varphi|| \wedge \Diamond Z) \\
||\mathbf{AG}\varphi|| &= \nu Z.(||\varphi|| \wedge \Box Z) \\
||\mathbf{E}(\varphi\mathbf{V}\psi)|| &= \nu Z.(||\psi|| \wedge (||\varphi|| \vee \Diamond Z)) \\
||\mathbf{A}(\varphi\mathbf{V}\psi)|| &= \nu Z.(||\psi|| \wedge (||\varphi|| \vee \Box Z))
\end{aligned}
$$

7 Example of Abstract Interpretation

In this section, we explain how our analysis applies to a simple safety-property verification of a program using an abstraction interpretation. The program is

```
/* 1 */
while(0 =< x){
    /* 2 */
    x = x+y;
    /* 3 */
}
/* 4 */
```

where x, y are integer variables. We aim to show that the line 4 in the program is not reachable if x and y are positive in the initial line 1.

To formalise the program as an interpretation, we take the following signature $\Sigma = (\mathbf{Prop}, \mathbf{Label})$ and the theory Δ.

$$\begin{aligned} \mathbf{Prop} &= \{\mathbf{isn't1},\ \mathbf{isn't4},\ (\mathbf{x} < \mathbf{0}),\ (\mathbf{y} < \mathbf{0})\} \\ \mathbf{Label} &= \{\mathbf{if}(\mathbf{pc} = \mathbf{1}),\ \mathbf{if}(\mathbf{pc} = \mathbf{2}),\ \mathbf{if}(\mathbf{pc} = \mathbf{3}),\ \mathbf{if}(\mathbf{0} =< \mathbf{x}),\ \mathbf{if}(\mathbf{x} < \mathbf{0}), \\ &\qquad \mathbf{pc} := \mathbf{2},\ \mathbf{pc} := \mathbf{3},\ \mathbf{pc} := \mathbf{4},\ \mathbf{x} := \mathbf{x} + \mathbf{y}\} \\ \Delta &= \emptyset \end{aligned}$$

Here, we give no condition among the above formulas. For example, we can have an interpretation m' such that $m'[\mathbf{if}(\mathbf{0} =< \mathbf{x})] = m'[\mathbf{if}(\mathbf{x} < \mathbf{0})]$.

The concrete interpretation $m \in \mathbf{LocOrd}_{lr}(\Sigma, U\mathbf{Pos_{CL}})$ we use must ofcourse match the intended semantics of the program we want to verify. We regard the program as a Kripke structure with the state set $\mathbf{W} = \{1, 2, 3, 4\} \times \mathbf{Z} \times \mathbf{Z}$. The numbers from 1 to 4 correspond to the lines so numbered in the program. Similarly to Example 2, the interpretation m is given by

$$\begin{aligned} &m\,* &&= \{\cdot\} \\ &m\,\mathbf{\Omega} &&= \wp(\mathbf{W}) \\ &m\,\mathbf{isn't1}(\cdot) &&= \{(c, a, b) \mid c \in \{2, 3, 4\}, a, b \in \mathbf{Z}\} \\ &m\,\mathbf{isn't4}(\cdot) &&= \{(c, a, b) \mid c \in \{1, 2, 3\}, a, b \in \mathbf{Z}\} \\ &m\,(\mathbf{x} < \mathbf{0})(\cdot) &&= \{(c, a, b) \mid c \in \{1, 2, 3, 4\}, a, b \in \mathbf{Z}, a < 0\} \\ &m\,(\mathbf{y} < \mathbf{0})(\cdot) &&= \{(c, a, b) \mid c \in \{1, 2, 3, 4\}, a, b \in \mathbf{Z}, b < 0\} \\ &m\,[\mathbf{if}(\mathbf{pc} = \mathbf{1})](X) &&= X \cup \{(c, a, b) \mid c \in \{2, 3, 4\}, a, b \in \mathbf{Z}\} \\ &m\,[\mathbf{if}(\mathbf{pc} = \mathbf{2})](X) &&= X \cup \{(c, a, b) \mid c \in \{1, 3, 4\}, a, b \in \mathbf{Z}\} \\ &m\,[\mathbf{if}(\mathbf{pc} = \mathbf{3})](X) &&= X \cup \{(c, a, b) \mid c \in \{1, 2, 4\}, a, b \in \mathbf{Z}\} \\ &m\,[\mathbf{if}(\mathbf{0} =< \mathbf{x})](X) &&= X \cup \{(c, a, b) \mid c \in \{1, 2, 3, 4\}, a, b \in \mathbf{Z}, a < 0\} \\ &m\,[\mathbf{if}(\mathbf{x} < \mathbf{0})](X) &&= X \cup \{(c, a, b) \mid c \in \{1, 2, 3, 4\}, a, b \in \mathbf{Z}, 0 \le a\} \\ &m\,[\mathbf{pc} := \mathbf{2}](X) &&= \{(c, a, b) \mid (2, a, b) \in X\} \\ &m\,[\mathbf{pc} := \mathbf{3}](X) &&= \{(c, a, b) \mid (3, a, b) \in X\} \\ &m\,[\mathbf{pc} := \mathbf{4}](X) &&= \{(c, a, b) \mid (4, a, b) \in X\} \\ &m\,[\mathbf{x} := \mathbf{x} + \mathbf{y}](X) &&= \{(c, a, b) \mid (c, a + b, b) \in X\} \end{aligned}$$

The safety property we want to show can be formally stated as the $R\mu$-formula σ:

$$\begin{aligned}
\sigma &= \vee \circ \langle \mathbf{isn't1}, \vee \circ \langle (\mathbf{x} < \mathbf{0}), \vee \circ \langle (\mathbf{y} < \mathbf{0}), \nu(\mathbf{isn't4}, \psi)\rangle\rangle\rangle \\
\psi &= \wedge \circ \langle \varphi_{1,4}, \wedge \circ \langle \varphi_{1,2}, \wedge \circ \langle \varphi_{2,3}, \wedge \circ \langle \varphi_{3,4}, \varphi_{3,2}\rangle\rangle\rangle\rangle \\
\varphi_{1,4} &= [\mathbf{if}(\mathbf{pc} = \mathbf{1})] \circ [\mathbf{if}(\mathbf{x} < \mathbf{0})] \circ [\mathbf{pc} := \mathbf{4}] \\
\varphi_{1,2} &= [\mathbf{if}(\mathbf{pc} = \mathbf{1})] \circ [\mathbf{if}(\mathbf{0} =< \mathbf{x})] \circ [\mathbf{pc} := \mathbf{2}] \\
\varphi_{2,3} &= [\mathbf{if}(\mathbf{pc} = \mathbf{2})] \circ [\mathbf{x} := \mathbf{x} + \mathbf{y}] \circ [\mathbf{pc} := \mathbf{3}] \\
\varphi_{3,4} &= [\mathbf{if}(\mathbf{pc} = \mathbf{3})] \circ [\mathbf{if}(\mathbf{x} < \mathbf{0})] \circ [\mathbf{pc} := \mathbf{4}] \\
\varphi_{3,2} &= [\mathbf{if}(\mathbf{pc} = \mathbf{3})] \circ [\mathbf{if}(\mathbf{0} =< \mathbf{x})] \circ [\mathbf{pc} := \mathbf{2}]
\end{aligned}$$

To show that the property holds is to show that $[\![\sigma]\!]_m$ is the greatest element of $U\mathbf{Pos_{CL}}(m*, m\mathbf{\Omega})$. However, we can not directly check if $w \in [\![\sigma]\!]_m(\cdot)$ for each $w \in \mathbf{W}$ as $\mathbf{W}$ is infinite.

Therefore, we construct an abstract interpretation for m according to Theorem 6. We use the predicate **pos** to abstract integers into boolean values.

$$\mathbf{pos}: \ \mathbf{Z} \to \{\mathbf{t}, \mathbf{f}\}$$
$$\mathbf{pos}(x) = \begin{cases} \mathbf{t} & (0 \le x) \\ \mathbf{f} & (x < 0) \end{cases}$$

Accordingly, we define the set $\mathbf{V}$ of abstract states and the abstraction relation $Q \subseteq \mathbf{W} \times \mathbf{V}$ by

$$\begin{aligned}
V &= \{1, 2, 3, 4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\} \\
Q &= \{((c, a, b), (c, \mathbf{pos}(a), \mathbf{pos}(b))) \mid (c, a, b) \in \mathbf{W}\}
\end{aligned}$$

The relation Q canonically gives rise to the adjunction $\alpha_{\mathbf{\Omega}} \dashv \gamma_{\mathbf{\Omega}} : \wp(\mathbf{W}) \to \wp(\mathbf{V})$.

$$\begin{aligned}
\alpha_{\mathbf{\Omega}}(X) &= \{w \in \mathbf{W} \mid \exists v \in X.(w, v) \in Q\} \\
\gamma_{\mathbf{\Omega}}(X) &= \{v \in \mathbf{V} \mid \forall w \in \mathbf{W}.(w, v) \in Q \Rightarrow w \in X\}
\end{aligned}$$

Together with this and $\gamma_* = \mathrm{id}_{\{\cdot\}}$, Theorem 6 gives the abstract interpretation $n \in \mathbf{LocOrd}_{lr}(\Sigma, U\mathbf{Pos_{CL}})$ for which $\gamma\colon\ m \to n$ is an abstraction.

$$\begin{aligned}
np &= \gamma_{\mathbf{\Omega}} \circ mp && \text{(for any } p \in \mathbf{Prop}\text{)} \\
n[a] &= \gamma_{\mathbf{\Omega}} \circ m[a] \circ \alpha_{\mathbf{\Omega}} && \text{(for any } a \in \mathbf{Label}\text{)}
\end{aligned}$$

Now it is directly checkable that $[\![\sigma]\!]_n$ is the greatest in $U\mathbf{Pos_{CL}}(n*, n\mathbf{\Omega})$ by checking every element of finite $\mathbf{W}$. The detail is shown in Appendix B. By Corollary 1, the formula σ satisfies $[\![\sigma]\!]_n \circ \gamma_* \le \gamma_{\mathbf{\Omega}} \circ [\![\sigma]\!]_m$, which is equivalent to $\alpha_{\mathbf{\Omega}} \circ [\![\sigma]\!]_n \le [\![\sigma]\!]_m$ in our case. The left hand side is the greatest in $U\mathbf{Pos_{CL}}(m*, m\mathbf{\Omega})$ by the definition of $\alpha_{\mathbf{\Omega}}$, hence so is $[\![\sigma]\!]_m$ as desired.

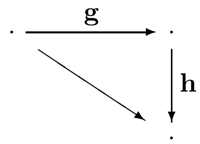
References

1. Michael Barr and Charles Wells. *Toposes, Triples and Theories*, volume 278 of *Grundlagen der Mathematischen Wissenschaften*. Springer-Verlag, Berlin, 1985.

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 David E. Long. Model checking and abstraction. *ACM Transactions on Programming Languages and Systems*, 16(5):1512–1542, September 1994.
4. P. Cousot and R. Cousot. Abstract interpretation: a unified lattice model for static analysis of programs by construction or approximation of fixpoints. In *Conference Record of the Fourth Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, pages 238–252, Los Angeles, California, 1977. ACM Press, New York, NY.
5. S. Graf and H. Saidi. Construction of abstract state graphs with pvs. In *Conference on Computer Aided Verification CAV'97*, LNCS 1254, Springer Verlag, 1997.
6. Chrysafis Hartonas. Duality for modal μ-logics. *Theoretical Computer Science*, 202(1–2):193–222, 28 July 1998.
7. G. M. Kelly. *Basic concepts of enriched category theory*, volume 64 of *London Mathematical Society lecture note series*. Cambridge University Press, 1982.
8. G. M. Kelly and A. J. Power. Adjunctions whose counits are coequalizers, and presentations of finitary enriched monads. *Journal of Pure and Applied Algebra*, 89:163–179, 1993.
9. Y. Kinoshita and J. Power. Lax naturality through enrichment. *Journal of Pure and Applied Algebra*, 112:53–72, 1996.
10. Yoshiki Kinoshita and John Power. A general completeness result in refinement. In *WADT'99*, LNCS 1827, Springer Verlag, 2000.
11. D. Kozen. Results on the propositional mu-calculus. *Theoretical Computer Science*, 27:333–354, 1983.
12. C. Loiseaux, S. Graf, J. Sifakis, A. Bouajjani, and S. Bensalem. Property preserving abstractions for the verification of concurrent systems. *Formal Methods in System Design Volume 6, Issue 1*, 1995.
13. Robin Milner. An algebraic definition of simulation between programs. In D. C. Cooper, editor, *Proceedings of the 2nd International Joint Conference on Artificial Intelligence*, pages 481–489, London, UK, September 1971. William Kaufmann.
14. Koki Nishizawa and John Power. Lawvere theories enriched over a general base. Programming Science Technical Report AIST-PS-2005-005, Research Center of Verification and Semantics, National Institute of Advanced Industrial Science and Technology, `http://unit.aist.go.jp/cvs/tr-data/ps05-005.pdf`, February 2005.
15. A. M. Pitts. Categorical logic. In S. Abramsky, D. M. Gabbay, and T. S. E. Maibaum, editors, *Handbook of Logic in Computer Science, Volume 5. Algebraic and Logical Structures*, chapter 2. Oxford University Press, 2000.
16. E.P. Robinson. Variations on algebra: monadicity and generalisations of equational theories. Computer Science Technical Report 6/94, University of Sussex, April 1994.
17. Klaus Schneider. *Verification of Reactive Systems*. Springer-Verlag, 2003.

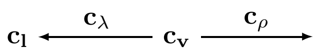
A Lawvere LocOrd-theory RMu

We define some examples of finitely presentable objects and arrows in **LocOrd**. Let 0 be the empty locally ordered category (no objects, no arrows). Let 1 be the locally ordered category with one object and one (identity) arrow. Let 2 be the locally ordered category with two objects $\mathbf{l}$ and $\mathbf{r}$. Let $\ulcorner \mathbf{l} \urcorner\colon 1 \to 2$ send the unique object of 1 to $\mathbf{l}$. Let $\ulcorner \mathbf{r} \urcorner\colon 1 \to 2$ send the unique object of 1 to $\mathbf{r}$. Let $\mathbf{2}$ be the locally ordered category with two objects and just one non-identity arrow. Let $\mathbf{s}\colon \mathbf{a} \to \mathbf{b}$ be the non-identity arrow in $\mathbf{2}$. Let $\ulcorner \mathbf{a} \urcorner\colon 1 \to \mathbf{2}$ send the unique object of 1 to $\mathbf{a}$. Let $\ulcorner \mathbf{b} \urcorner\colon 1 \to \mathbf{2}$ send the unique object of 1 to $\mathbf{b}$. Let $\ulcorner \mathbf{a}, \mathbf{b} \urcorner\colon 2 \to \mathbf{2}$ send $\mathbf{l}$ to $\mathbf{a}$ and send $\mathbf{r}$ to $\mathbf{b}$. Let $\ulcorner \mathrm{u} \urcorner$ be the unique functor from X to 1 in $\mathbf{LocOrd}_f$ for any X. Let $\mathbf{3}$ be the locally ordered category with three objects whose non-identity arrows are arranged as in the triangle. (This diagram commutes.)



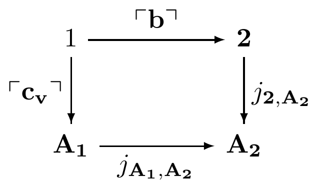
Let $\ulcorner \mathbf{g} \urcorner\colon \mathbf{2} \to \mathbf{3}$ send $\mathbf{s}$ to $\mathbf{g}$. Let $\ulcorner \mathbf{h} \urcorner\colon \mathbf{2} \to \mathbf{3}$ send $\mathbf{s}$ to $\mathbf{h}$. Let $\ulcorner \mathbf{h} \circ \mathbf{g} \urcorner\colon \mathbf{2} \to \mathbf{3}$ send $\mathbf{s}$ to $\mathbf{h} \circ \mathbf{g}$.

Let $\mathbf{A_1}$ be the locally ordered category with three objects and two non-identity arrows as follows.



Let $\ulcorner \mathbf{c_v} \urcorner\colon 1 \to \mathbf{A_1}$ send the unique object of 1 to $\mathbf{c_v}$. Let $\ulcorner id_{\mathbf{c_v}} \urcorner\colon \mathbf{2} \to \mathbf{A_1}$ send $\mathbf{s}$ to the identity arrow on $\mathbf{c_v}$. Let $\ulcorner \mathbf{c_{l,r}} \urcorner\colon 2 \to \mathbf{A_1}$ send $\mathbf{l}$ to $\mathbf{c_l}$ and send $\mathbf{r}$ to $\mathbf{c_r}$. Let $\ulcorner \mathbf{c}_\lambda \urcorner\colon \mathbf{2} \to \mathbf{A_1}$ send $\mathbf{s}$ to $\mathbf{c}_\lambda$. Let $\ulcorner \mathbf{c}_\rho \urcorner\colon \mathbf{2} \to \mathbf{A_1}$ send $\mathbf{s}$ to $\mathbf{c}_\rho$.

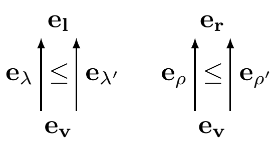
We define $\mathbf{A_2}$ by the following pushout.



Let $\ulcorner \mathbf{c} \circ \mathbf{s} \urcorner\colon \mathbf{A_1} \to \mathbf{A_2}$ send $\mathbf{c}_\lambda$ to $\mathbf{c}_\lambda \circ \mathbf{s}$ and send $\mathbf{c}_\rho$ to $\mathbf{c}_\rho \circ \mathbf{s}$.

Let $\mathbf{A_3}$ be the locally ordered category with two objects $\mathbf{i_a}$ and $\mathbf{i_b}$ and arrows $\mathbf{i_s}, \mathbf{i_{s'}}\colon \mathbf{i_a} \to \mathbf{i_b}$ subject to inequality $\mathbf{i_s} \leq \mathbf{i_{s'}}$. Let $\ulcorner \mathbf{i_s} \urcorner\colon \mathbf{2} \to \mathbf{A_3}$ send $\mathbf{s}$ to $\mathbf{i_s}$. Let $\ulcorner \mathbf{i_{s'}} \urcorner\colon \mathbf{2} \to \mathbf{A_3}$ send $\mathbf{s}$ to $\mathbf{i_{s'}}$.

Let $\mathbf{A_4}$ be the following locally ordered category.



Let $\ulcorner \mathbf{e}_{\lambda,\rho} \urcorner\colon \mathbf{A_1} \to \mathbf{A_4}$ send $\mathbf{c}_\lambda$ to $\mathbf{e}_\lambda$ and send $\mathbf{c}_\rho$ to $\mathbf{e}_\rho$. Let $\ulcorner \mathbf{e}_{\lambda',\rho'} \urcorner\colon \mathbf{A_1} \to \mathbf{A_4}$ send $\mathbf{c}_\lambda$ to $\mathbf{e}_{\lambda'}$ and send $\mathbf{c}_\rho$ to $\mathbf{e}_{\rho'}$.

We define $\mathbf{A_5}$ and $\mathbf{A_6}$ by the following pushouts, respectively.

$$\begin{array}{ccc} \mathbf{2} & \xrightarrow{\ulcorner \mathbf{h} \circ \mathbf{g} \urcorner} & \mathbf{3} \\ {\scriptstyle \ulcorner \mathbf{i_s} \urcorner}\downarrow & & \downarrow{\scriptstyle j_{\mathbf{3},\mathbf{A_5}}} \\ \mathbf{A_3} & \xrightarrow[j_{\mathbf{A_3},\mathbf{A_5}}]{} & \mathbf{A_5} \end{array} \qquad \begin{array}{ccc} \mathbf{2} & \xrightarrow{\ulcorner \mathbf{h} \circ \mathbf{g} \urcorner} & \mathbf{3} \\ {\scriptstyle \ulcorner \mathbf{i_{s'}} \urcorner}\downarrow & & \downarrow{\scriptstyle j_{\mathbf{3},\mathbf{A_6}}} \\ \mathbf{A_3} & \xrightarrow[j_{\mathbf{A_3},\mathbf{A_6}}]{} & \mathbf{A_6} \end{array}$$

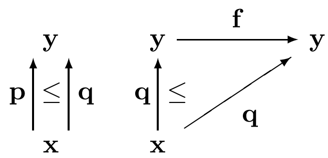
Let $\mathbf{A_7}$ be the locally ordered category with two objects $\mathbf{x}$, $\mathbf{y}$ and non-identity arrows generated from $\mathbf{p}\colon \mathbf{x} \to \mathbf{y}$ and $\mathbf{f}\colon \mathbf{y} \to \mathbf{y}$. Let $\ulcorner \mathbf{f} \urcorner\colon \mathbf{2} \to \mathbf{A_7}$ send $\mathbf{s}$ to $\mathbf{f}$. Let $\ulcorner \mathbf{p} \urcorner\colon \mathbf{2} \to \mathbf{A_7}$ send $\mathbf{s}$ to $\mathbf{p}$. Let $\ulcorner \mathbf{x} \urcorner\colon 1 \to \mathbf{A_7}$ send the unique object of 1 to $\mathbf{x}$. Let $\ulcorner \mathbf{x}, \mathbf{y} \urcorner\colon 2 \to \mathbf{A_7}$ send $\mathbf{l}$ to $\mathbf{x}$ and send $\mathbf{r}$ to $\mathbf{y}$.

We define $\mathbf{A_8}$ by the following pushout.

$$\begin{array}{ccc} 1 & \xrightarrow{\ulcorner \mathbf{b} \urcorner} & \mathbf{2} \\ {\scriptstyle \ulcorner \mathbf{x} \urcorner}\downarrow & & \downarrow{\scriptstyle j_{\mathbf{2},\mathbf{A_8}}} \\ \mathbf{A_7} & \xrightarrow[j_{\mathbf{A_7},\mathbf{A_8}}]{} & \mathbf{A_8} \end{array}$$

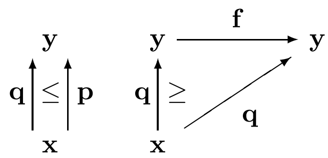
Let $\ulcorner \mathbf{p} \circ \mathbf{s}, \mathbf{f} \urcorner\colon \mathbf{A_7} \to \mathbf{A_8}$ send $\mathbf{p}$ to $\mathbf{p} \circ \mathbf{s}$ and send $\mathbf{f}$ to $\mathbf{f}$.

Let $\mathbf{A_9}$ be the locally ordered category with two objects $\mathbf{x}$, $\mathbf{y}$ and non-identity arrows generated from $\mathbf{p}, \mathbf{q}\colon \mathbf{x} \to \mathbf{y}$ and $\mathbf{f}\colon \mathbf{y} \to \mathbf{y}$ subject to inequalities $\mathbf{p} \leq \mathbf{q}$ and $\mathbf{f} \circ \mathbf{q} \leq \mathbf{q}$.



Let $j_{\mathbf{2},\mathbf{A_9}}\colon \mathbf{2} \to \mathbf{A_9}$ send $\mathbf{s}$ to $\mathbf{q}$. Let $j_{\mathbf{A_7},\mathbf{A_9}}\colon \mathbf{A_7} \to \mathbf{A_9}$ send $\mathbf{p}$ to $\mathbf{p}$ and send $\mathbf{f}$ to $\mathbf{f}$.

Let $\mathbf{A_{10}}$ be the locally ordered category with objects $\mathbf{x}$, $\mathbf{y}$ and non-identity arrows generated from $\mathbf{p}, \mathbf{q}\colon \mathbf{x} \to \mathbf{y}$ and $\mathbf{f}\colon \mathbf{y} \to \mathbf{y}$ subject to inequalities $\mathbf{q} \leq \mathbf{p}$ and $\mathbf{q} \leq \mathbf{f} \circ \mathbf{q}$.

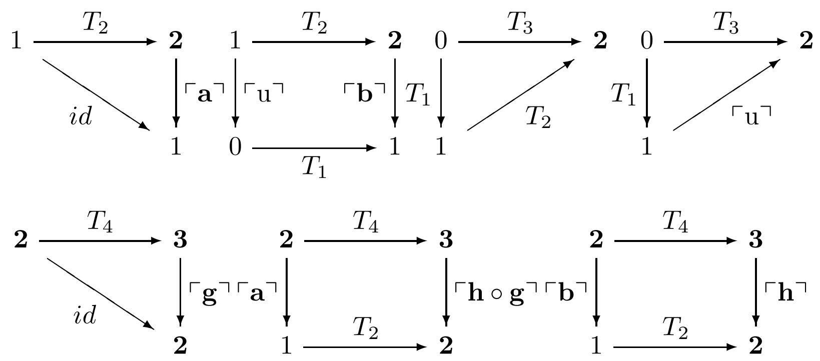


Let $j_{\mathbf{2},\mathbf{A_{10}}}\colon \mathbf{2} \to \mathbf{A_{10}}$ send $\mathbf{s}$ to $\mathbf{q}$. Let $j_{\mathbf{A_7},\mathbf{A_{10}}}\colon \mathbf{A_7} \to \mathbf{A_{10}}$ send $\mathbf{p}$ to $\mathbf{p}$ and send $\mathbf{f}$ to $\mathbf{f}$.

We define Lawvere **LocOrd**-theory **RMu** corresponding to the formal system $R\mu$. Let **RMu** be freely generated from $(\mathbf{LocOrd})_f^{\mathrm{op}}$ by adding the following operations subject to the following diagrams. We can also reformulate by a single operation for multiple operations that have a common domain. However, since it is difficult to understand the correspondence between the reformulated Lawvere **LocOrd**-theory and the formal system, we do not so.

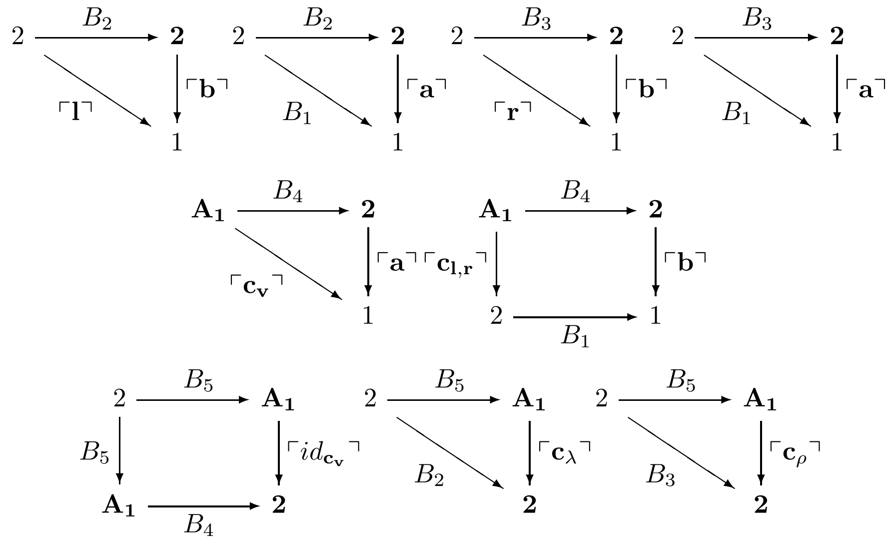
Terminal

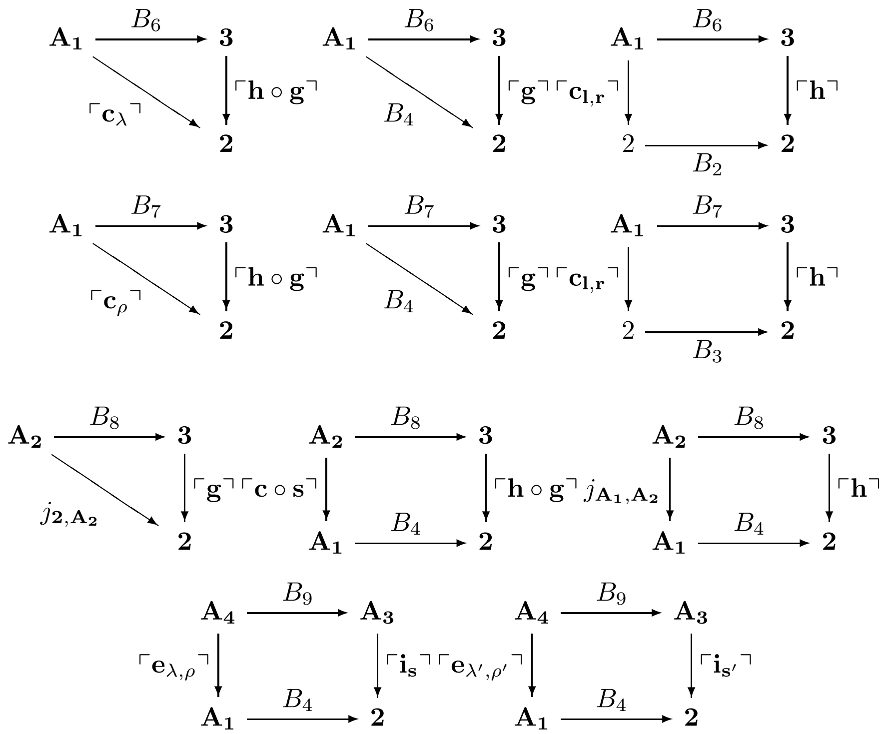
$$\begin{aligned} T_1 &: 0 \to 1 \\ T_2 &: 1 \to \mathbf{2} \\ T_3 &: 0 \to \mathbf{2} \\ T_4 &: \mathbf{2} \to \mathbf{3} \end{aligned}$$



Binary product

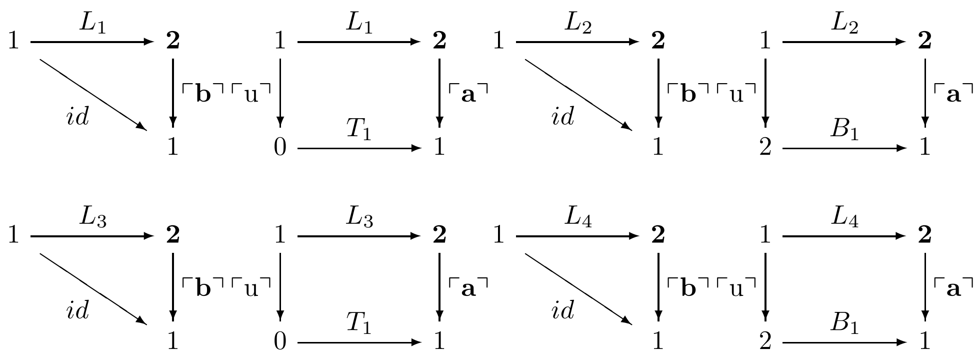
$$\begin{aligned} B_1 &: 2 \to 1 \\ B_2 &: 2 \to \mathbf{2} \\ B_3 &: 2 \to \mathbf{2} \\ B_4 &: \mathbf{A_1} \to \mathbf{2} \\ B_5 &: 2 \to \mathbf{A_1} \\ B_6 &: \mathbf{A_1} \to \mathbf{3} \\ B_7 &: \mathbf{A_1} \to \mathbf{3} \\ B_8 &: \mathbf{A_2} \to \mathbf{3} \\ B_9 &: \mathbf{A_4} \to \mathbf{A_3} \end{aligned}$$

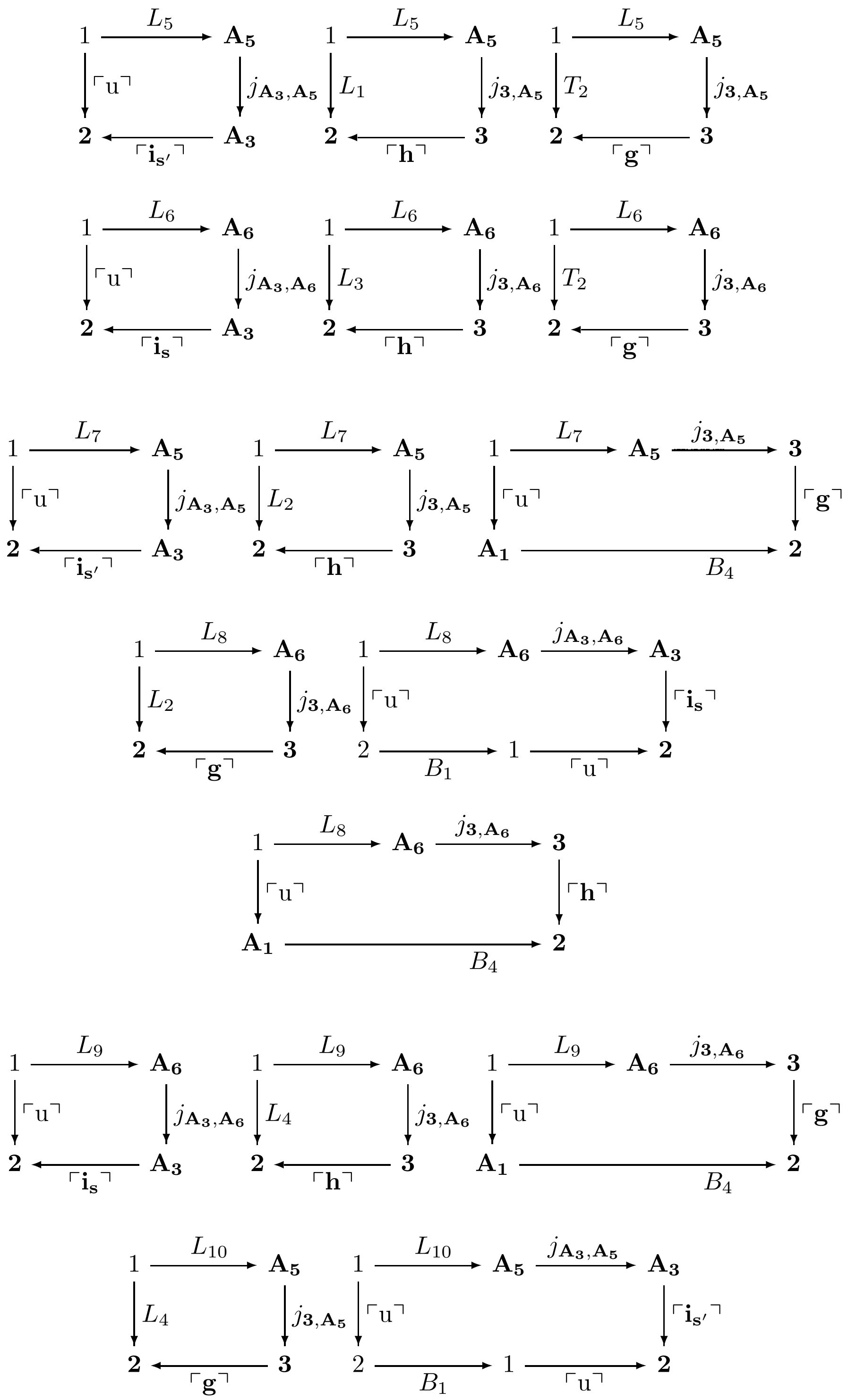


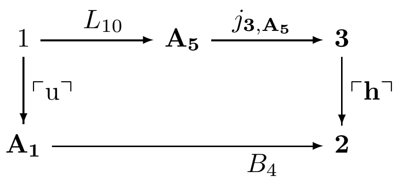


Lattice

$$
\begin{aligned}
L_1 &\colon 1 \to \mathbf{2}\\
L_2 &\colon 1 \to \mathbf{2}\\
L_3 &\colon 1 \to \mathbf{2}\\
L_4 &\colon 1 \to \mathbf{2}\\
L_5 &\colon 1 \to \mathbf{A_5}\\
L_6 &\colon 1 \to \mathbf{A_6}\\
L_7 &\colon 1 \to \mathbf{A_5}\\
L_8 &\colon 1 \to \mathbf{A_6}\\
L_9 &\colon 1 \to \mathbf{A_6}\\
L_{10} &\colon 1 \to \mathbf{A_5}
\end{aligned}
$$

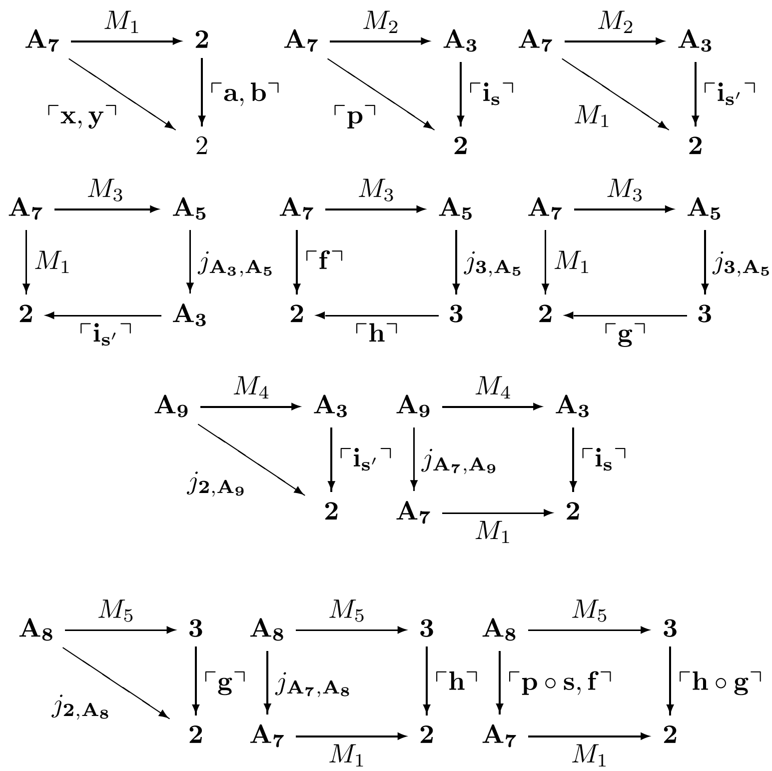



1 L5 A5 ⌜u⌝ j A3,A5 2 ⌜is′⌝ A3
1 L5 A5 L1 j3,A5 2 ⌜h⌝ 3
1 L5 A5 T2 j3,A5 2 ⌜g⌝ 3
1 L6 A6 ⌜u⌝ jA3,A6 2 ⌜is⌝ A3
1 L6 A6 L3 j3,A6 2 ⌜h⌝ 3
1 L6 A6 T2 j3,A6 2 ⌜g⌝ 3
1 L7 A5 ⌜u⌝ jA3,A5 2 ⌜is′⌝ A3
1 L7 A5 L2 j3,A5 2 ⌜h⌝ 3
1 L7 A5 j3,A5 3 ⌜u⌝ ⌜g⌝ A1 B4 2
1 L8 A6 L2 j3,A6 2 ⌜g⌝ 3
1 L8 A6 jA3,A6 A3 ⌜u⌝ ⌜is⌝ 2 B1 1 ⌜u⌝ 2
1 L8 A6 j3,A6 3 ⌜u⌝ ⌜h⌝ A1 B4 2
1 L9 A6 ⌜u⌝ jA3,A6 2 ⌜is⌝ A3
1 L9 A6 L4 j3,A6 2 ⌜h⌝ 3
1 L9 A6 j3,A6 3 ⌜u⌝ ⌜g⌝ A1 B4 2
1 L10 A5 L4 j3,A5 2 ⌜g⌝ 3
1 L10 A5 jA3,A5 A3 ⌜u⌝ ⌜is′⌝ 2 B1 1 ⌜u⌝ 2



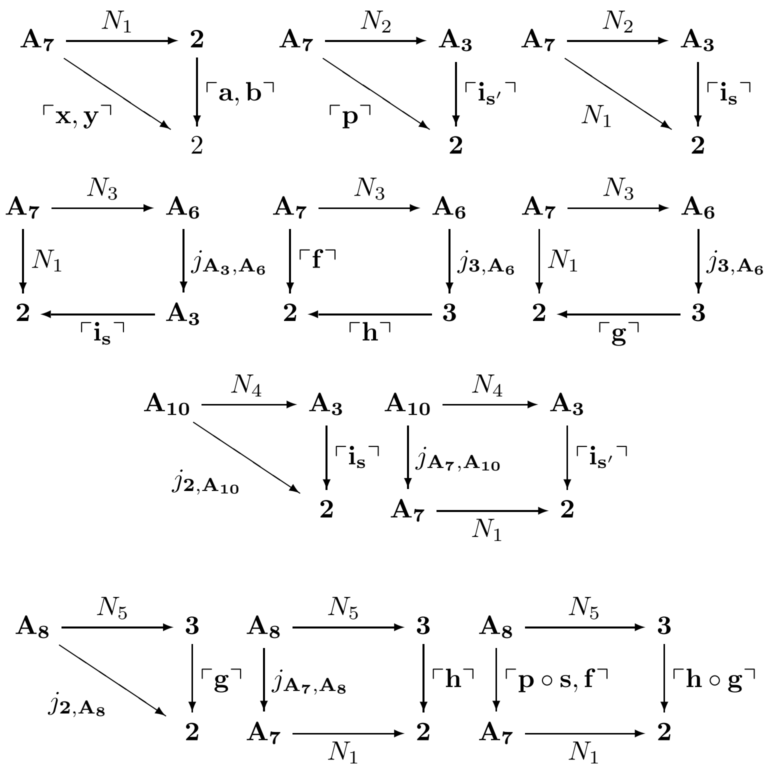
Least fixed point of restricted formula

$$
\begin{aligned}
M_1 &\colon\ \mathbf{A_7} \to \mathbf{2}\\
M_2 &\colon\ \mathbf{A_7} \to \mathbf{A_3}\\
M_3 &\colon\ \mathbf{A_7} \to \mathbf{A_5}\\
M_4 &\colon\ \mathbf{A_9} \to \mathbf{A_3}\\
M_5 &\colon\ \mathbf{A_8} \to \mathbf{3}
\end{aligned}
$$



Greatest fixed point of restricted formula

$$
\begin{aligned}
N_1 &\colon\ \mathbf{A_7} \to \mathbf{2}\\
N_2 &\colon\ \mathbf{A_7} \to \mathbf{A_3}\\
N_3 &\colon\ \mathbf{A_7} \to \mathbf{A_6}\\
N_4 &\colon\ \mathbf{A_{10}} \to \mathbf{A_3}\\
N_5 &\colon\ \mathbf{A_8} \to \mathbf{3}
\end{aligned}
$$



B Model Checking for Finite Set of States

In this section, we show that $[\![\sigma]\!]_n$ in Section 7 is a greatest element in $U\mathbf{Pos}_{\mathbf{CL}}(n*, n\mathbf{\Omega})$. By Theorem 6, we construct n as follows.

$$
\begin{array}{ll}
n* & = \{\cdot\} \\
n\mathbf{\Omega} & = \wp(\mathbf{V}) \\
n\mathbf{isn't1}(\cdot) & = \{2,3,4\} \times \{\mathbf{t},\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\} \\
n\mathbf{isn't4}(\cdot) & = \{1,2,3\} \times \{\mathbf{t},\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\} \\
n(\mathbf{x} < \mathbf{0})(\cdot) & = \{1,2,3,4\} \times \{\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\} \\
n(\mathbf{y} < \mathbf{0})(\cdot) & = \{1,2,3,4\} \times \{\mathbf{t},\mathbf{f}\} \times \{\mathbf{f}\} \\
n[\mathbf{if}(\mathbf{pc} = \mathbf{1})](X) & = X \cup (\{2,3,4\} \times \{\mathbf{t},\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\}) \\
n[\mathbf{if}(\mathbf{pc} = \mathbf{2})](X) & = X \cup (\{1,3,4\} \times \{\mathbf{t},\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\}) \\
n[\mathbf{if}(\mathbf{pc} = \mathbf{3})](X) & = X \cup (\{1,2,4\} \times \{\mathbf{t},\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\}) \\
n[\mathbf{if}(\mathbf{0} =< \mathbf{x})](X) & = X \cup (\{1,2,3,4\} \times \{\mathbf{f}\} \times \{\mathbf{t},\mathbf{f}\}) \\
n[\mathbf{if}(\mathbf{x} < \mathbf{0})](X) & = X \cup (\{1,2,3,4\} \times \{\mathbf{t}\} \times \{\mathbf{t},\mathbf{f}\}) \\
n[\mathbf{pc} := \mathbf{2}](X) & = \{(c,a,b) \mid c \in \{1,2,3,4\}, a,b \in \{\mathbf{t},\mathbf{f}\}, (2,a,b) \in X\} \\
n[\mathbf{pc} := \mathbf{3}](X) & = \{(c,a,b) \mid c \in \{1,2,3,4\}, a,b \in \{\mathbf{t},\mathbf{f}\}, (3,a,b) \in X\} \\
n[\mathbf{pc} := \mathbf{4}](X) & = \{(c,a,b) \mid c \in \{1,2,3,4\}, a,b \in \{\mathbf{t},\mathbf{f}\}, (4,a,b) \in X\}
\end{array}
$$

$$
\begin{aligned}
n[\mathbf{x} := \mathbf{x} + \mathbf{y}](X) = {} & \{(c, \mathbf{t}, \mathbf{t}) \mid c \in \{1,2,3,4\}, (c, \mathbf{t}, \mathbf{t}) \in X\} \cup \\
& \{(c, \mathbf{t}, \mathbf{f}) \mid c \in \{1,2,3,4\}, (c, \mathbf{t}, \mathbf{f}), (c, \mathbf{f}, \mathbf{f}) \in X\} \cup \\
& \{(c, \mathbf{f}, \mathbf{t}) \mid c \in \{1,2,3,4\}, (c, \mathbf{t}, \mathbf{t}), (c, \mathbf{f}, \mathbf{t}) \in X\} \cup \\
& \{(c, \mathbf{f}, \mathbf{f}) \mid c \in \{1,2,3,4\}, (c, \mathbf{f}, \mathbf{f}) \in X\}
\end{aligned}
$$

Combining the above functions, we get $[\![\varphi_{1,4}]\!]_n$, $[\![\varphi_{1,2}]\!]_n$, $[\![\varphi_{2,3}]\!]_n$, $[\![\varphi_{3,4}]\!]_n$, $[\![\varphi_{3,2}]\!]_n$, and $[\![\psi]\!]_n$ as follows.

$$
\begin{aligned}
\varphi_{1,4} &= [\mathbf{if}(\mathbf{pc} = \mathbf{1})] \circ [\mathbf{if}(\mathbf{x} < \mathbf{0})] \circ [\mathbf{pc} := \mathbf{4}] \\
[\![\varphi_{1,4}]\!]_n(X) &= (\{2,3,4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}) \cup \\
& \quad \{(1, \mathbf{t}, \mathbf{t}), (1, \mathbf{t}, \mathbf{f})\} \cup \\
& \quad \{(1, \mathbf{f}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (4, \mathbf{f}, b) \in X\}
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{1,2} &= [\mathbf{if}(\mathbf{pc} = \mathbf{1})] \circ [\mathbf{if}(\mathbf{0} =< \mathbf{x})] \circ [\mathbf{pc} := \mathbf{2}] \\
[\![\varphi_{1,2}]\!]_n(X) &= (\{2,3,4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}) \cup \\
& \quad \{(1, \mathbf{f}, \mathbf{t}), (1, \mathbf{f}, \mathbf{f})\} \cup \\
& \quad \{(1, \mathbf{t}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (2, \mathbf{t}, b) \in X\}
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{2,3} &= [\mathbf{if}(\mathbf{pc} = \mathbf{2})] \circ [\mathbf{x} := \mathbf{x} + \mathbf{y}] \circ [\mathbf{pc} := \mathbf{3}] \\
[\![\varphi_{2,3}]\!]_n(X) &= (\{1,3,4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}) \cup \\
& \quad \{(2, a, b) \mid a, b \in \{\mathbf{t}, \mathbf{f}\}, (3, a, b), (3, b, b) \in X\}
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{3,4} &= [\mathbf{if}(\mathbf{pc} = \mathbf{3})] \circ [\mathbf{if}(\mathbf{x} < \mathbf{0})] \circ [\mathbf{pc} := \mathbf{4}] \\
[\![\varphi_{3,4}]\!]_n(X) &= (\{1,2,4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}) \cup \\
& \quad \{(3, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{f})\} \cup \\
& \quad \{(3, \mathbf{f}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (4, \mathbf{f}, b) \in X\}
\end{aligned}
$$

$$
\begin{aligned}
\varphi_{3,2} &= [\mathbf{if}(\mathbf{pc} = \mathbf{3})] \circ [\mathbf{if}(\mathbf{0} =< \mathbf{x})] \circ [\mathbf{pc} := \mathbf{2}] \\
[\![\varphi_{3,2}]\!]_n(X) &= (\{1,2,4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}) \cup \\
& \quad \{(3, \mathbf{f}, \mathbf{t}), (3, \mathbf{f}, \mathbf{f})\} \cup \\
& \quad \{(3, \mathbf{t}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (2, \mathbf{t}, b) \in X\}
\end{aligned}
$$

$$
\begin{aligned}
\psi &= \wedge \circ \langle \varphi_{1,4}, \wedge \circ \langle \varphi_{1,2}, \wedge \circ \langle \varphi_{2,3}, \wedge \circ \langle \varphi_{3,4}, \varphi_{3,2} \rangle\rangle\rangle\rangle \\
[\![\psi]\!]_n(X) &= (\{4\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}) \cup \\
& \quad \{(1, \mathbf{f}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (4, \mathbf{f}, b) \in X\} \cup \\
& \quad \{(1, \mathbf{t}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (2, \mathbf{t}, b) \in X\} \cup \\
& \quad \{(2, a, b) \mid a, b \in \{\mathbf{t}, \mathbf{f}\}, (3, a, b), (3, b, b) \in X\} \cup \\
& \quad \{(3, \mathbf{f}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (4, \mathbf{f}, b) \in X\} \cup \\
& \quad \{(3, \mathbf{t}, b) \mid b \in \{\mathbf{t}, \mathbf{f}\}, (2, \mathbf{t}, b) \in X\}
\end{aligned}
$$

Next, we compute $[\![\nu(\mathbf{isn't4}, \psi)]\!]_n$. By the structure of $\mathbf{Pos_{CL}}$, $[\![\nu(\mathbf{isn't4}, \psi)]\!]_n(\cdot)$ is the greatest fixed point of the following function $F\colon \wp(\mathbf{V}) \to \wp(\mathbf{V})$.

$$
F(X) = [\![\mathbf{isn't4}]\!]_n(\cdot) \cap [\![\psi]\!]_n(X)
$$

Since $\mathbf{V}$ is a finite set, we can compute the value as follows. Since $F^4(\mathbf{V}) = F^5(\mathbf{V})$, the greatest fixed point $[\![\nu(\mathbf{isn't4}, \psi)]\!]_n(\cdot)$ is $F^5(\mathbf{V}) = \{(1, \mathbf{t}, \mathbf{t}), (2, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{t})\}$.

$F^0(\mathbf{V}) = \mathbf{V}$
$F^1(\mathbf{V}) = \{1, 2, 3\} \times \{\mathbf{t}, \mathbf{f}\} \times \{\mathbf{t}, \mathbf{f}\}$
$F^2(\mathbf{V}) = \{(1, \mathbf{t}, \mathbf{t}), (1, \mathbf{t}, \mathbf{f}), (2, \mathbf{t}, \mathbf{t}), (2, \mathbf{t}, \mathbf{f}), (2, \mathbf{f}, \mathbf{t}), (2, \mathbf{f}, \mathbf{f}), (3, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{f})\}$
$F^3(\mathbf{V}) = \{(1, \mathbf{t}, \mathbf{t}), (1, \mathbf{t}, \mathbf{f}), (2, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{f})\}$
$F^4(\mathbf{V}) = \{(1, \mathbf{t}, \mathbf{t}), (2, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{t})\}$
$F^5(\mathbf{V}) = \{(1, \mathbf{t}, \mathbf{t}), (2, \mathbf{t}, \mathbf{t}), (3, \mathbf{t}, \mathbf{t})\}$

Therefore, we can easily prove that $[\![\sigma]\!]_n(\cdot) = \mathbf{V}$ for the following σ.

$$\sigma = \vee \circ \langle \mathbf{isn't1}, \vee \circ \langle (\mathbf{x} < \mathbf{0}), \vee \circ \langle (\mathbf{y} < \mathbf{0}), \nu(\mathbf{isn't4}, \psi) \rangle \rangle \rangle$$

不動点論理と抽象解釈のための代数構造 (in English)
(算譜科学研究速報)
発行日：2005 年 6 月 15 日
編集・発行：独立行政法人産業技術総合研究所関西センター尼崎事業所
システム検証研究センター
同連絡先：〒661-0974 兵庫県尼崎市若王寺 3-11-46
e-mail：informatics-inquiry@m.aist.go.jp

Algebraic Structure for a Fixed Point Logic and Abstract Interpretation
(Programming Science Technical Report)
June 15, 2005
Research Center for Verification and Semantics (CVS)
AIST Kansai, Amagasaki Site
National Institute of Advanced Industrial Science and Technology (AIST)
3-11-46 Nakouji, Amagasaki, Hyogo, 661-0974, Japan
e-mail: informatics- inquiry@m.aist.go.jp