On algorithmic expressivity of finite-variable fragments of intuitionistic modal logics

Mikhail Rybakov

Institute for Information Transmission Problems, RAS

HSE University

Tver State University

Dmitry Shkatov

University of the Witwatersrand, Johannesburg

SCAN 2023

16 June, 2023

Motivation

- Whenever we have a logic with a computationally hard satisfiability or validity problem, we want to find out if it has less computationally demanding fragments.
- On the one hand, the classical logic **CL** and the modal logics **K5**, **K45**, and **S5** are all NP-complete, but their finite-variable fragments are all in P.
- On the other, for most modal propositional logics, the single-variable or even the variable-free fragment is as hard as the full logic. E.g., **K**, **KT**, **KB**, **KTB**, **K4**, **S4**, **GL**, **Grz**, etc.
- Very often, a finite-variable is as hard as the full logic since the logic can be poly-time embedded into the fragment in a 'structure-preserving' way ... so, 'structure-preserving' poly-time embeddability is a stronger property.

This talk

We show that modal intuitionistic logics **FS** and **MIPC** are poly-time embeddable into their single-variable fragments.

Language

Modal intuitionistic formulas:

$$\varphi \quad := \quad p \mid \bot \mid (\varphi \wedge \varphi) \mid (\varphi \vee \varphi) \mid (\varphi \to \varphi) \mid \Box\varphi \mid \Diamond\varphi$$

Standard abbreviations:

$$\begin{array}{lcl} \neg\varphi & = & \varphi \to \bot; \\ \varphi \leftrightarrow \psi & = & (\varphi \to \psi) \wedge (\psi \to \varphi). \end{array}$$

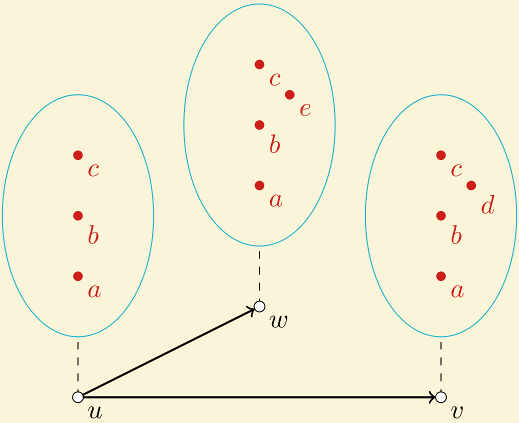
Semantics

- A *Kripke frame* is a pair $\mathfrak{F} = \langle W, R \rangle$ where $W \neq \varnothing$ and R is a partial order on W.
- An **FS**-*frame* is a triple $\boldsymbol{F} = \langle W, R, \delta \rangle$, where $\langle W, R \rangle$ is a Kripke frame and δ is a map associating with each $w \in W$ a structure $\langle \Delta_w, S_w \rangle$, with $\Delta_w \neq \varnothing$ and $S_w \subseteq \Delta_w \times \Delta_w$ subject to

$$v \in R(w) \ \Rightarrow \ \Delta_w \subseteq \Delta_v \quad \text{and} \quad S_w \subseteq S_v$$

- An **FS**-frame $\boldsymbol{F} = \langle W, R, \delta \rangle$ is an **MIPC**-*frame* if $S_w = \Delta_w \times \Delta_w$, for every $w \in W$.

FS-frames: an example



S is an equivalence at each world, so this is an **MIPC**-frame.

Semantics

- A *valuation* on an **FS**-frame $\langle W, R, \delta\rangle$ is a map V such that $V(w,p) \subseteq \Delta_w$ and

$$v \in R(w) \implies V(w,p) \subseteq V(v,p).$$

- The pair $\mathfrak{M} = \langle \boldsymbol{F}, V\rangle$, where $\boldsymbol{F}$ is an **FS**-frame and V a valuation on $\boldsymbol{F}$, is called an **FS**-*model*. An **MIPC**-*model* is an **FS**-model over an **MIPC**-frame.

Semantics: the satisfaction relation

- $\mathfrak{M}, w, x \models p$ if $x \in V(w, p)$;
- $\mathfrak{M}, w, x \not\models \bot$;
- $\mathfrak{M}, w, x \models \varphi_1 \wedge \varphi_2$ if $\mathfrak{M}, w, x \models \varphi_1$ and $\mathfrak{M}, w, x \models \varphi_2$;
- $\mathfrak{M}, w, x \models \varphi_1 \vee \varphi_2$ if $\mathfrak{M}, w, x \models \varphi_1$ or $\mathfrak{M}, w, x \models \varphi_2$;
- $\mathfrak{M}, w, x \models \varphi_1 \to \varphi_2$ if $\mathfrak{M}, v, x \not\models \varphi_1$ or $\mathfrak{M}, v, x \models \varphi_2$ whenever $v \in R(w)$;
- $\mathfrak{M}, w, x \models \Diamond\varphi_1$ if $\mathfrak{M}, w, y \models \varphi_1$, for some $y \in S_w(x)$;
- $\mathfrak{M}, w, x \models \Box\varphi_1$ if $\mathfrak{M}, v, y \models \varphi_1$ whenever $v \in R(w)$ and $y \in S_v(x)$.

Semantics and logics

- A formula φ is *true* in a model $\mathfrak{M}$ if $\mathfrak{M}, w, x \models \varphi$, for every world w of $\mathfrak{M}$ and every point x of w.
- A formula φ is *valid* an **FS**-frame $\mathfrak{F}$ if φ is true in every model over $\mathfrak{F}$.
- **FS** is the set of formulas valid on every **FS**-frame.
- **MIPC** is the set of formulas valid on every **MIPC**-frame.

Let φ be a formula and $f \notin var\,\varphi$. Define

- $\varphi^f = [f/\bot]\varphi$;
- $F_1 = \Diamond^{\leqslant md\,\varphi} f \to f$;
- $F_2 = f \to \Box^{\leqslant md\,\varphi} f$;
- $F_3 = \bigwedge\limits_{p \in var\,\varphi} \Box^{\leqslant md\,\varphi}(f \to p)$;
- $F = F_1 \wedge F_2 \wedge F_3$.

Lemma

Let φ be a formula, $f \notin var\,\varphi$, and $L \in \{\mathbf{FS}, \mathbf{MIPC}\}$. Then,

$$\varphi \in L \iff F \to \varphi^f \in L.$$

Since φ^f and F are both positive, the map $e\colon \varphi \mapsto (F \to \varphi^f)$ embeds **FS** and **MIPC** into their own positive fragments.

Embedding into single-variable fragment

We next define a polytime computable function $\cdot^*$ from the set of positive formulas to the set of one-variable positive formulas and show that, for $L \in \{\mathbf{FS}, \mathbf{MIPC}\}$ and every positive φ,

$$\varphi^* \in L \quad \Longleftrightarrow \quad \varphi \in L.$$

Hence, for every φ,

$$\varphi \in L \quad \Longleftrightarrow \quad e(\varphi) \in L \quad \Longleftrightarrow \quad \big(e(\varphi)\big)^* \in L.$$

Simulation of variables

We next define formulas that we substitute for propositional variables of φ. These formulas, except G_1, G_2, and G_3, are divided into 'levels', indexed by elements of $\mathbb{N}$; formulas of level 0 are denoted A_i^0 or B_i^0, those of level 1, by A_i^1 and B_i^1, etc.

First, G_1, G_2, and G_3, as well as formulas of levels 0 and 1:

$$\begin{array}{rcl} G_1 & = & \Diamond p; \\ G_2 & = & \Diamond p \to p; \\ G_3 & = & p \to \Box p; \\ A_1^0 & = & G_2 \to G_1 \vee G_3; \\ A_2^0 & = & G_3 \to G_1 \vee G_2; \\ B_1^0 & = & G_1 \to G_2 \vee G_3; \\ B_2^0 & = & A_1^0 \wedge A_2^0 \wedge B_1^0 \to G_1 \vee G_2 \vee G_3; \end{array}$$

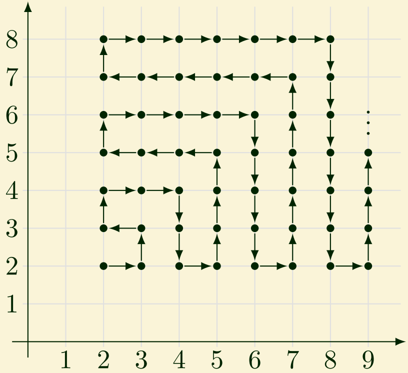
$$\begin{array}{rcl} A_1^1 & = & A_1^0 \wedge A_2^0 \to B_1^0 \vee B_2^0; \\ A_2^1 & = & A_1^0 \wedge B_1^0 \to A_2^0 \vee B_2^0; \\ A_3^1 & = & A_1^0 \wedge B_2^0 \to A_2^0 \vee B_1^0; \\ B_1^1 & = & A_2^0 \wedge B_1^0 \to A_1^0 \vee B_2^0; \\ B_2^1 & = & A_2^0 \wedge B_2^0 \to A_1^0 \vee B_1^0; \\ B_3^1 & = & B_1^0 \wedge B_2^0 \to A_1^0 \vee A_2^0. \end{array}$$

Simulation of variables

Suppose that $k \geqslant 1$ and that we have defined

$$A_1^k, \ldots, A_{n_k}^k \quad \text{and} \quad B_1^k, \ldots, B_{n_k}^k$$

Define a linear order $\prec$ on $(\mathbb{N} \setminus \{0,1\}) \times (\mathbb{N} \setminus \{0,1\})$:



Simulation of variables

Suppose g enumerates pairs according to $\prec$. Define

$$A^{k+1}_{g(i,j)} \;=\; A^k_1 \to B^k_1 \vee A^k_i \vee B^k_j; \qquad B^{k+1}_{g(i,j)} \;=\; B^k_1 \to A^k_1 \vee A^k_i \vee B^k_j,$$

and define n_{k+1} be the number of the formulas of the form A^{k+1}_i.

Observation:

$$n_{k+1} \;=\; (n_k - 1)^2.$$

Let

$$l_0 \;=\; |A^0_1| + |B^0_1| + |A^0_2| + |B^0_2|.$$

Lemma

There exists $k_0 \in \mathbb{N}$ such that $n_k > l_0 \cdot 5^k$ whenever $k \geqslant k_0$.

Simulation of variables

Let φ be a positive formula with $var\,\varphi = \{p_1, \ldots, p_s\}$. Let k_φ be the least integer k such that $|\varphi| < l_0 \cdot 5^k$. By Lemma,

$$n_{k_\varphi + k_0} > l_0 \cdot 5^{k_\varphi + k_0}.$$

Hence,

$$n_{k_\varphi + k_0} > l_0 \cdot 5^{k_\varphi + k_0} > 5^{k_0} \cdot |\varphi| > |\varphi| \geqslant s.$$

Lastly, define φ^* to be the result of the substitution

$$A_r^{k_\varphi + k_0} \vee B_r^{k_\varphi + k_0} \quad \text{for} \quad p_r,$$

for each $r \in \{1, \ldots, s\}$ (this substitution is well defined since $n_{k_\varphi + k_0} > s$).

The reduction is poly-time

Lemma

For every $k \geqslant 0$ and every $i \in \{1, \ldots, n_k\}$,

$$|A_i^k| < l_0 \cdot 5^k \quad \textit{and} \quad |B_i^k| < l_0 \cdot 5^k.$$

Lemma

The formula φ^* is computable in time polynomial in $|\varphi|$.

Proof. We show that $|\varphi^*|$ is polynomial in $|\varphi|$. Since k_φ is the least integer k such that $|\varphi| < l_0 \cdot 5^k$, surely $l_0 \cdot 5^{k_\varphi - 1} \leqslant |\varphi|$, and so

$$l_0 \cdot 5^{k_\varphi + k_0} \leqslant 5^{k_0+1}|\varphi|.$$

By Lemma, for every $i \in \{1, \ldots, n_{k_\varphi + k_0}\}$,

$$|A_i^{k_\varphi + k_0}| < l_0 \cdot 5^{k_\varphi + k_0} \leqslant 5^{k_0+1}|\varphi| \;\&\; |B_i^{k_\varphi + k_0}| < l_0 \cdot 5^{k_\varphi + k_0} \leqslant 5^{k_0+1}|\varphi|.$$

Hence, $|\varphi^*| < 2 \cdot 5^{k_0+1}|\varphi|^2$.

Main result

Lemma

Let $L \in \{\mathbf{FS}, \mathbf{MIPC}\}$. Then, for every positive formula φ,

$$\varphi \in L \quad \Longleftrightarrow \quad \varphi^* \in L.$$

Theorem

Let $L \in \{\mathbf{FS}, \mathbf{MIPC}\}$. Then, there exists a stucture-preserving polynomial-time computable function embedding L into its own positive one-variable fragment.

Corollary

Let $L \in \{\mathbf{FS}, \mathbf{MIPC}\}$. Then, the positive one-variable fragment of L is polytime-equivalent to L.

Thank you!