ON ALGORITHMIC EXPRESSIVITY OF FINITE-VARIABLE FRAGMENTS OF
INTUITIONISTIC MODAL LOGICS

MIKHAIL RYBAKOV AND DMITRY SHKATOV

1. Introduction

Modal and intuitionistic propositional logics are often poly-time embeddable into their own fragments with a few variables (typically, zero, one, or two), and similar embeddings are sometimes constructed of fragments of logics with special properties into finite-variable fragments of those logics. The literature on the topic is quite extensive [2, 27, 11, 12, 4, 29] and includes contributions by the authors of this paper [3, 14, 15, 16, 17, 18, 20, 19, 21, 22, 23, 24, 25].

As a result, the validity problem for such fragments is as computationally hard as the validity problem for the full logic. (In general, modal and superintuitionistic propositional logics, even linearly approximable ones, may have arbitrarily hard fragments with a few variables since, for every set \( A \subseteq \mathbb{N} \), one can construct [26] a linearly approximable logic whose fragment with a few variables typically zero, one, or two) recursively encodes \( A \). We obtain here similar embeddings for the intuitionistic modal logics \( \text{FS} \) and \( \text{MIPC} \), introduced by, respectively, Fisher Servi [7] and Prior [13]. These logics have been introduced as counterparts of bimodal propositional logics, and can also be viewed as fragments of the predicate intuitionistic logic \( \text{QInt} \) (for details, see [10]); we note that this is not the only approach to constructing modal intuitionistic logics, cf. [5, 6, 28]. The complexity of \( \text{FS} \) and \( \text{MIPC} \) remains unresolved, but the results presented here show that single-variable fragments of these logics have the same complexity as the full logics.

2. Preliminaries

The intuitionistic modal language contains a countable set \( P \) of propositional variables, the constant \( \bot \), binary connectives \( \odot, \land, \) and \( \rightarrow \), and unary modal connectives \( \Diamond \) and \( \Box \). Formulas are defined in the usual way. A formula is positive if it does not contain occurrences of \( \bot \). The set of propositional variables of a formula \( \varphi \) is denoted by \( \text{var} \varphi \). The result of substituting a formula \( \psi \) for a variable \( p \) into a formula \( \varphi \) is denoted by \([\psi/p] \varphi\). The modal depth of a formula \( \varphi \), denoted by \( md \varphi \), is the maximal number of nested modal connectives in \( \varphi \). The length of a formula \( \varphi \), defined as the number of symbols in \( \varphi \) (with the binary encoding of variables), is denoted by \( |\varphi| \).

We define the logics \( \text{FS} \) and \( \text{MIPC} \) semantically. A Kripke frame is a pair \( \mathcal{F} = (W, R) \) where \( W \) is a non-empty set of worlds and \( R \) is a partial order on \( W \). An \( \text{FS-frame} \) is a triple \( \mathcal{F} = (W, R, \delta) \), where \( (W, R) \) is a Kripke frame and \( \delta \) is a map associating with each \( w \in W \) a structure \( (\Delta_w, S_w) \), with \( \Delta_w \) being a non-empty set of points and \( S_w \) a binary relation on \( \Delta_w \) such that, for every \( w, v \in W \),

\[ v \in R(w) \Rightarrow \Delta_w \subseteq \Delta_v \text{ and } S_w \subseteq S_v. \]

An \( \text{FS-frame} \) \( \mathcal{F} = (W, R, \delta) \) is an \( \text{MIPC-frame} \) if \( S_w = \Delta_w \times \Delta_w \), for every \( w \in W \). A valuation on an \( \text{FS-frame} \) \( (W, R, \delta) \) is a map associating with each \( w \in W \) and each \( p \in P \) a subset \( V(w, p) \) of \( \Delta_w \) in such a way that

\[ v \in R(w) \Rightarrow V(w, p) \subseteq V(v, p). \]

The pair \( \mathfrak{M} = (\mathcal{F}, V) \), where \( \mathcal{F} \) is an \( \text{FS-frame} \) and \( V \) a valuation on \( \mathcal{F} \), is called an \( \text{FS-model} \). An \( \text{MIPC-model} \) is an \( \text{FS-model} \) over an \( \text{MIPC-frame} \). The truth-relation \( \models \) is defined by recursion (here, \( \mathfrak{M} \) is a model, \( w \in W \), \( x \in \Delta_w \), and \( \varphi \) is a formula):

- \( \mathfrak{M}, w, x \models p \) \iff \( x \in V(w, p) \) if \( p \in P \);
- \( \mathfrak{M}, w, x \not\models \bot \);
- \( \mathfrak{M}, w, x \models \varphi_1 \odot \varphi_2 \) \iff \( \mathfrak{M}, w, x \models \varphi_1 \) and \( \mathfrak{M}, w, x \models \varphi_2 \);
- \( \mathfrak{M}, w, x \models \varphi_1 \land \varphi_2 \) \iff \( \mathfrak{M}, w, x \models \varphi_1 \) or \( \mathfrak{M}, w, x \models \varphi_2 \);
- \( \mathfrak{M}, w, x \models \varphi \rightarrow \varphi_2 \) \iff \( \mathfrak{M}, v, x \not\models \varphi_1 \) or \( \mathfrak{M}, v, x \models \varphi_2 \) whenever \( v \in R(w) \);
- \( \mathfrak{M}, w, x \models \Diamond \varphi_1 \) \iff \( \mathfrak{M}, w, y \models \varphi_1 \), for some \( y \in S_w(x) \);
- \( \mathfrak{M}, w, x \models \Box \varphi_1 \) \iff \( \mathfrak{M}, v, y \models \varphi_1 \), whenever \( v \in R(w) \) and \( y \in S_v(x) \).
A formula \( \varphi \) is true in a model \( M \) (notation: \( M \models \varphi \)) if \( M, w, x \models \varphi \), for every world \( w \) of \( M \) and every point \( x \) of \( w \). A formula \( \varphi \) is valid an FS-frame \( \mathfrak{F} \) if \( \varphi \) is true in every model over \( \mathfrak{F} \). Logics FS and MIPC are defined as sets of formulas valid on, respectively, every FS-frame and every MIPC-frame.

3. Main results

In this section, we prove that logics FS and MIPC are polynomial-time embeddable into their own fragments with a single propositional variable. We first poly-time embed these logics into their own positive fragments. Let \( \varphi \) be a formula and \( f \in \mathcal{P} \setminus \text{var } \varphi \). Define

\[
\varphi^f = [f/\bot] \varphi; \quad F_1 = \Diamond \leq^m \varphi \rightarrow f; \quad F_2 = f \rightarrow \Box \leq^m \varphi; \quad F_3 = \bigwedge_{p \in \text{var } \varphi} \square \leq^m \varphi(f \rightarrow p),
\]

and put \( F = F_1 \circ F_2 \circ F_3 \).

**Lemma 1.** Let \( \varphi \) be a formula, \( f \in \mathcal{P} \setminus \text{var } \varphi \), and \( L \in \{\text{FS, MIPC}\} \). Then,

\[
\varphi \in L \iff F \rightarrow \varphi^f \in L.
\]

Since \( \varphi^f \) and \( F \) are both positive, the map \( e: \varphi \mapsto (F \rightarrow \varphi^f) \) embeds FS and MIPC into their own positive fragments.

We next define a polytime computable function \( * \) from the set of positive formulas to the set of one-variable positive formulas and show that, for \( L \in \{\text{FS, MIPC}\} \) and every positive \( \varphi \),

\[
\varphi^* \in L \iff \varphi \in L.
\]

Hence, for every \( \varphi \),

\[
\varphi \in L \iff e(\varphi) \in L \iff e(\varphi)^* \in L.
\]

The formula \( \varphi^* \) shall be obtain from \( \varphi \) using a substitution. We next define the formulas that shall be substituted for propositional variables of \( \varphi \). 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 \( A_0 \) or \( B_0 \), those of level 1, by \( A_1 \) and \( B_1 \), etc. We begin with \( G_1, G_2 \), and \( G_3 \), as well as formulas of levels 0 and 1:

\[
\begin{align*}
G_1 &= \Diamond p; \\
G_2 &= \Diamond p \rightarrow p; \\
G_3 &= p \rightarrow \Box p; \\
A_0 &= G_2 \rightarrow G_1 \land G_3; \\
A_1 &= A_0 \circ A_0 \rightarrow B_0 \land B_2; \\
B_0 &= G_1 \rightarrow G_2 \land G_3; \\
B_1 &= B_0 \circ B_0 \rightarrow A_0 \land A_2.
\end{align*}
\]

We proceed by recursion. Let \( k \geq 1 \). Suppose the formulas \( A_1, \ldots, A_n \) and \( B_1, \ldots, B_n \) have been defined, with \( n_k \) being the number of formulas of the form \( A_k \) and, also, the number of formulas of the form \( B_k \) (e.g., if \( k = 1 \), then \( n_k = 3 \); the recursive definition for the cases where \( k \geq 2 \) is to be given). Define a linear order \( \prec \) on the set \( \mathbb{N} \setminus \{0, 1\} \times (\mathbb{N} \setminus \{0, 1\}) \) as in the following picture, so that \( (i, j) \prec (i', j') \) if, and only if, there exists a path along one or more arrows from \( (i, j) \) to \( (i', j') \):
We can then define an enumeration $g$ of the pairs $(i, j) \in (\mathbb{N} \setminus \{0,1\}) \times (\mathbb{N} \setminus \{0,1\})$ according to $\prec$, i.e., so that $g(2, 2) = 1$, $g(3, 2) = 2$, $g(3, 3) = 3$, $g(2, 3) = 4$, etc. Now, for every $i, j \in \{2, \ldots, n_k\}$, define

$$A^{k+1}_{g(i, j)} = A^k_i \rightarrow B^k_1 \land A^k_j \land B^k_j; \quad B^{k+1}_{g(i, j)} = B^k_i \rightarrow A^k_i \land A^k_j \land B^k_j,$$

and let $n_{k+1}$ be the number of the formulas of the form $A^{k+1}_i$ (which is the same as the number of formulas of the form $B^{k+1}_i$) so defined; notice that $n_{k+1} = (n_k - 1)^2$. This completes the recursive definition of $A^k_i$ and $B^k_j$.

Next, put

$$l_0 = |A^0_0| + |B^0_1| + |A^0_2| + |B^0_2|.$$

Lemma 2. There exists $k_0 \in \mathbb{N}$ such that $n_k > l_0 \cdot 5^k$ whenever $k \geq k_0$.

Now, let $\varphi$ be a positive formula with $\text{var} \varphi = \{p_1, \ldots, p_s\}$. Let $k_{\varphi}$ be the least integer $k$ such that $|\varphi| < l_0 \cdot 5^k$. By Lemma 2, $n_{k_{\varphi} + k_0} > l_0 \cdot 5^{k_{\varphi} + k_0}$, hence,

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

Lastly, define $\varphi^*$ to be the result of substituting into $\varphi$, for every $r \in \{1, \ldots, s\}$, the formula $A^{k_{\varphi} + k_0}_r \land B^{k_{\varphi} + k_0}_r$ for the variable $p_r$ (this substitution is well defined since $n_{k_{\varphi} + k_0} > s$).

We next show that $\varphi^*$ is poly-time computable from $\varphi$.

Lemma 3. For every $k \geq 0$ and every $i \in \{1, \ldots, n_k\}$,

$$|A^k_i| < l_0 \cdot 5^k \quad \text{and} \quad |B^k_i| < l_0 \cdot 5^k.$$

Lemma 4. The formula $\varphi^*$ is computable in time polynomial in $|\varphi|$.

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

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

By Lemma 3, for every $i \in \{1, \ldots, n_{k_{\varphi} + k_0}\}$,

$$|A^{k_{\varphi} + k_0}_i| < l_0 \cdot 5^{k_{\varphi} + k_0} \leq 5^{k_0 + 1} |\varphi| \quad \text{and} \quad |B^{k_{\varphi} + k_0}_i| < l_0 \cdot 5^{k_{\varphi} + k_0} \leq 5^{k_0 + 1} |\varphi|.$$

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

To obtain the desired result, it remains to show the following:

Lemma 5. Let $L \in \{\text{FS, MIPC}\}$. Then, for every positive formula $\varphi$,

$$\varphi \in L \iff \varphi^* \in L.$$ 

From Lemmas 1, 4, and 5, we immediately obtain the following:

Theorem 6. Let $L \in \{\text{FS, MIPC}\}$. Then, there exists a polynomial-time computable function embedding $L$ into its own positive one-variable fragment.

Corollary 7. Let $L \in \{\text{FS, MIPC}\}$. Then, the positive one-variable fragment of $L$ is polytime-equivalent to $L$.

The results presented here are not immediately applicable to obtaining the computational complexity of finite-variable fragments of intuitionistic modal logics since the complexity of full logics remains unknown (we are only aware of decidability results [9, 31, 30, 1, 8] for modal intuitionistic logics).

Acknowledgements. The work on this paper, carried out at the Institute for Information Transmission Problems of the Russian Academy of Sciences, has been supported by Russian Science Foundation, Project 21-18-00195.
References


(M. Rybakov) IITP RAS, Moscow, Russia and HSE University, Moscow, Russia

(D. Shkatov) University of the Witwatersrand, Johannesburg, South Africa

Email address, M. Rybakov: m.rybakov@mail.ru
Email address, D. Shkatov: shkatov@gmail.com