Deciding Modal Logics through Relational Translations into GF^2

10.08.2004

Hans de Nivelle,

Max-Planck Institut für Informatik, Saarbrücken, Germany.

This is joint work with Stéphane Demri,

Laboratoire Spécification et Vérification, Cachan, France,

Aim of our work:

- Translating many modal logics (regular grammar logics with converse) into the guarded fragment by 'fine-tuning' the relational translation method.

Motivation of our work:

- Extending the scope of the relational translation method for automated theorem proving. This gives a modular approach to theorem proving for numerous modal logics.

- Gaining more insight into regular grammar logics with converse.

Multimodal Propositional Logic:

Let PROP be the set of propositional variables, let Σ be some alphabet. Modal formulas are recursively defined as follows:

- A propositional variable $p \in \mathrm{PROP}$ is a modal formula,
- if ψ is a modal formula, then $\neg\psi$ is also a modal formula,
- if ψ_1, ψ_2 are modal formulas, then $\psi_1 \vee \psi_2,\ \psi_1 \wedge \psi_2,\ \psi_1 \rightarrow \psi_2,\ \psi_1 \leftrightarrow \psi_2$ are also modal formulas,
- if ψ is a modal formula, and $a \in \Sigma$, then $[a]\ \psi$ and $\langle a \rangle\ \psi$ are also modal formulas.

Kripke Semantics for Multimodal Logic

Modal formulas are interpreted in Kripke models. A Σ-model $\mathcal{M} = (W, R, V)$ is an ordered triple, of which W is a non-empty set, R is a function that assigns to each $a \in \Sigma$ a subset of $W \times W$, and V is a function that assigns to each $p \in \mathrm{PROP}$ a subset of W.

If $w \in W$, then

- $\mathcal{M}, w \models p$ iff $w \in R(p)$,
- $\mathcal{M}, w \models \neg\, \psi$ iff not $\mathcal{M}, w \models \psi$,
- $\mathcal{M}, w \models \psi_1 \vee \psi_2$ iff $\mathcal{M}, w \models \psi_1$ or $\mathcal{M}, w \models \psi_2$,
- $\mathcal{M}, w \models [a]\, \psi$ iff for all $w' \in W$, if $(w, w') \in R(a)$, then $\mathcal{M}, w' \models \psi$,
- $\mathcal{M}, w \models \langle a \rangle\, \psi$ iff there is a $w' \in W$, s.t. $(w, w') \in R(a)$, and $\mathcal{M}, w' \models \psi$.

Characterizations of Modal Logics

Different modal logics can be characterized by different subsets of Kripke models:

Logic K	(all Kripke models)
Logic B	For $a \in \Sigma$, relations $R(a)$ are symmetric,
Logic $S4$	For $a \in \Sigma$, relations $R(a)$ are transitive and reflexive,
Logic $K4$	For $a \in \Sigma$, relations $R(a)$ are transitive,
Logic $S5$	For $a \in \Sigma$, relations $R(a)$ are equivalence relations.

Modal Logic and First-Order Logic:

We assume that there is a unique unary predicate symbol $\mathbf{P}$ associated to every $p \in \mathrm{PROP}$, and that there is a relation symbol $\mathbf{R}_a$ associated to every $a \in \Sigma$.

- To every Σ-model (W, R, V), one can associate a first-order model (W, V') as follows: For each $a \in \Sigma$, $V'(\mathbf{R}_a) = R(a)$, and for each $p \in \mathrm{PROP}$, $V'(\mathbf{P}) = V(p)$.

  We call (W, V') the first-order model associated to (W, R, V).

- To every first-order model (W, V'), interpreting the $\mathbf{P}$ and $\mathbf{R}_a$, one can associate a Σ-model (W, V) as follows: For each $a \in \Sigma$, $R(a) = V'(\mathbf{R}_a)$, and for each $p \in \mathbf{PROP}$, $V(p) = V'(\mathbf{P})$. We call (W, R, V) the Σ-model associated to (W, V').

Relational Translation (with recycling of variables):

Using the correspondence between the modal language and the first-order language, one can define:

$t(p, \alpha, \beta) = \mathbf{P}(\alpha)$,
$t(\neg\psi, \alpha, \beta) = \neg\ t(\psi, \alpha, \beta)$,
$t(\psi_1 \wedge \psi_2) = t(\psi_1, \alpha, \beta) \wedge t(\psi_2, \alpha, \beta)$,
$t(\psi_1 \vee \psi_2) = t(\psi_1, \alpha, \beta) \vee t(\psi_2, \alpha, \beta)$,
$t(\psi_1 \rightarrow \psi_2) = t(\psi_1, \alpha, \beta) \rightarrow t(\psi_2, \alpha, \beta)$,
$t(\psi_1 \leftrightarrow \psi_2) = t(\psi_1, \alpha, \beta) \leftrightarrow t(\psi_2, \alpha, \beta)$,
$t(\langle a \rangle\ \psi, \alpha, \beta) = \exists\beta\ [\ \mathbf{R}_a(\alpha, \beta) \wedge t(\psi, \beta, \alpha)\ ]$,
$t([a]\ \psi, \alpha, \beta) = \forall\beta\ [\ \mathbf{R}_a(\alpha, \beta) \rightarrow t(\psi, \beta, \alpha)\ ]$.

Theorem: Let $\mathcal{M}$ be a Σ-model, let $\mathcal{M}'$ be a first-order model, s.t. $\mathcal{M}$ and $\mathcal{M}'$ are associated models of each other. Then $\mathcal{M}, w \models \psi$ iff $\mathcal{M}'[w \leftarrow \alpha] \models t(\psi, \alpha, \beta)$.

Theorem: Let $\mathcal{L}$ be a modal logic, defined by a restriction on Kripke frames.

Let $F_{\mathcal{L}}$ be a closed first-order formula, s.t. for each pair of associated models $\mathcal{M}, \mathcal{M}'$, we have $\mathcal{M}' \models F_{\mathcal{L}}$ iff $\mathcal{M}$ is a Kripke model allowed by the logic $\mathcal{L}$.

Let ψ be a modal formula. Then ψ is satisfiable in $\mathcal{L}$ iff $F \wedge \exists \alpha \; t(\psi, \alpha, \beta)$ is satisfiable in FOL.

Decidable Fragments of First-Order Logic

Definition: A formula F is in the guarded fragment if

1. F is function free,
2. every quantification in F has form $\forall \overline{x}\ a \rightarrow \Phi$, or $\exists \overline{x}\ a \wedge \Phi$, where a is an atom, s.t. all free variables of Φ occur in a.

Definition A formula F is in the 2-variable fragment if

1. F is function free,
2. F contains at most two variables.

Theorem: For a modal formula ψ, $t(\psi, \alpha, \beta)$ is both in the guarded fragment and in the 2-variable fragment.

Theorem: Both for the 2-variable fragment and the guarded fragment, the satisfiability problem is decidable. For the 2-variable fragment, it is NEXPTIME-complete. For the guarded fragment (when the arity of the symbols is fixed), it is EXPTIME-complete.

This gives a nice way of deciding satsfiability in modal logic K and some other modal logics:

If one wants to decide whether formula ψ is satisfiable in modal logic $\mathcal{L}$, then test satisfiability of $F_{\mathcal{L}} \wedge \exists\alpha\ t(\psi, \alpha, \beta)$.

The method works when $F_{\mathcal{L}}$ is in a decidable fragment.

Unfortunately, many (simple) modal logics $\mathcal{L}$ have $F_{\mathcal{L}}$ outside of these fragments. An example is S4, which is characterized by transitivity:

$$\forall w_1 w_2 w_3 \; \mathbf{R}_a(w_1, w_2) \wedge \mathbf{R}_a(w_2, w_3) \rightarrow \mathbf{R}_a(w_1, w_3).$$

So, is everything lost?

Do we have to give up in despair?

Example: Modal Logic S4

A formula is in negation normal form if

it does not contain $\leftrightarrow$ and $\rightarrow$, and $\neg$ is applied only on propositional variables.

Improved Relational Translation for S4:

$$
\begin{aligned}
&t_{S4}(p, \alpha, \beta) = \mathbf{P}(\alpha),\\
&t_{S4}(\neg p, \alpha, \beta) = \neg\mathbf{P}(\alpha),\\
&t_{S4}(\psi_1 \wedge \psi_2) = t_{S4}(\psi_1, \alpha, \beta) \wedge t_{S4}(\psi_2, \alpha, \beta),\\
&t_{S4}(\psi_1 \vee \psi_2) = t_{S4}(\psi_1, \alpha, \beta) \vee t_{S4}(\psi_2, \alpha, \beta),\\
&t_{S4}(\langle a\rangle\ \psi, \alpha, \beta) = \exists\beta\ \mathbf{R}_a(\alpha, \beta) \wedge t_{S4}(\psi, \beta, \alpha),\\
&t_{S4}([a]\ \psi, \alpha, \beta) =\\
&\qquad X(\alpha) \wedge\\
&\qquad \forall\alpha\beta\ \ X(\alpha) \rightarrow \mathbf{R}_a(\alpha, \beta) \rightarrow X(\beta) \wedge \qquad\qquad (X \text{ is a new symbol})\\
&\qquad \forall\alpha\ \ X(\alpha) \rightarrow t_{S4}(\psi, \alpha, \beta).
\end{aligned}
$$

For a modal formula ψ in NNF, $t_{S4}(\psi, \alpha, \beta)$ is **(1)** in the guarded fragment, and **(2)** in the 2-variable fragment.

Theorem: For a modal formula ψ in NNF, ψ is S4-satisfiable iff $t_{S4}(\psi, \alpha, \beta)$ is FO-satisfiable

proof: $(\Rightarrow)$
if ψ is S4-satisfiable, then ψ has a Σ-model $\mathcal{M} = (W, R, V)$, in which each R_a is transitive and reflexive. First construct a first-order model $\mathcal{M}' = (W, V')$, as the first-order model associated to $\mathcal{M}$.

The interpretations of the X predicates can be obtained as follows: Each X predicate was obtained by translating some formula of form $[a]\ \psi$. Then $V'(X) = \{w \in W \mid \mathcal{M}, w \models [a]\ \psi\}$.

proof: $(\Leftarrow)$

If $t_{S4}(\psi, \alpha, \beta)$ is FO-satisfiable, then there are a model $\mathcal{M}' = (W, V')$, and a $w \in W$, s.t. $\mathcal{M}'[w \leftarrow \alpha] \models t_{S4}(\psi, \alpha, \beta)$.

Let $\mathcal{M} = (W, R, V)$ be the Σ-model associated to $\mathcal{M}'$. Let R^* be the transitive, reflexive closure of R. Let $\mathcal{M}^* = (W, R^*, V)$.

Apply induction on ψ to prove $\mathcal{M}^*, w \models \psi$.

All cases are identical to the cases for the standard relational translation. The only exception is the $[a]$-case.

Suppose that ψ has form $[a]\varphi$.

Assume that $(w, w') \in R^*(a)$. By the way R^* is constructed, there is a chain (with possibly $n = 0$)

$$w = v_0, \ldots, v_n = w', \quad (v_0, v_1) \in V(R), \ldots, (v_{n-1}, v_n) \in V(R),$$

Since $\mathcal{M}'[w \leftarrow \alpha] \models t_{S4}([a]\varphi, \alpha, \beta)$, we have

- $\mathcal{M}'[w \leftarrow \alpha] \models X(\alpha)$,
- $\mathcal{M}' \qquad\qquad \models \forall\alpha\beta \;\; X(\alpha) \rightarrow \mathbf{R}_a(\alpha, \beta) \rightarrow X(\beta)$,
- $\mathcal{M}' \qquad\qquad \models \forall\alpha \;\; X(\alpha) \rightarrow t_{S4}(\varphi, \alpha, \beta)$.

By 'unfolding' we obtain

- $\mathcal{M}'[w' \leftarrow \alpha] \models t_{S4}(\psi, \alpha, \beta)$.

Now it is possible to apply induction and to obtain $\mathcal{M}^*, w' \models \psi$.

Regular Grammar Logics with Converse

What is the 'special' property of S4 that makes this method work? The closure property of S4 (reflexivity + transitivity) allows a simple (Horn clause) description of the worlds that are reachable from a given world.

For S4, this is the conjunction of formulas $t_{S4}([a]\ \psi, \alpha, \beta) =$

$$X(\alpha),$$

$$\forall \alpha\beta \;\; X(\alpha) \to \mathbf{R}_a(\alpha, \beta) \to X(\beta), \qquad \forall \alpha \;\; X(\alpha) \to t_{S4}(\psi, \alpha, \beta).$$

In an X-minimal model, X is true in exactly the worlds that are reachable from α.

Grammar Logics

A Semi-Thue system S over alphabet Σ is a set of rules of form $u \rightarrow v$, where both $u, v \in \Sigma^*$. A Semi-Thue system is context free if for each rule $u \rightarrow v$, we have $u \in \Sigma$.

To a Semi-Thue system S belongs a rewrite relation $\Rightarrow^*$, defined as the smallest reflexive, transitive relation satisfying: If $(u \rightarrow v) \in S$, then $u_1 \cdot u \cdot u_2 \Rightarrow^* u_1 \cdot v \cdot u_2$.

For a symbol $a \in \Sigma$, the language generated by a, written as $L_S(a)$ is defined as $\{v \mid a \Rightarrow^* v\}$.

Given a Σ-model $\mathcal{M} = (W, R, V)$, the interpretations $R(a)$ can be extended to words over Σ^* as follows:

- $R(\epsilon) = \{(w, w) \mid w \in W\}$.
- $R(u \cdot v) = \{(w_1, w_3) \mid \exists w_2 \in W, \text{ such that } (w_1, w_2) \in R(u) \text{ and } (w_2, w_3) \in R(v)\}$.

A Σ-model (W, R, V) satisfies a rule $u \rightarrow v$ if $R(v) \subseteq R(u)$. A Σ-model satisfies a semi-Thue system S if it satisfies all its rules.

Example: Transitivity of a can be expressed by the rule $a \rightarrow aa$.

Reflexivity of a can be expressed by the rule $a \rightarrow \epsilon$.

S4 is characterized by $S = \{\ a \rightarrow aa, \quad a \rightarrow \epsilon\ \}$.

Converses

Definition: Let Σ be an alphabet. We call a function $\bar{\cdot}$ (of signature $\Sigma \to \Sigma$) a converse mapping if for all $a \in \Sigma$,

$$\overline{a} \neq a \text{ and } \overline{\overline{a}} = a.$$

Lemma: Given some alphabet Σ and a partition $\bar{\cdot}$, Σ can be partitioned into two disjoint sets Σ^+ and Σ^-, s.t.

- for all $a \in \Sigma^+$, $a \in \Sigma^-$,
- for all $a \in \Sigma^-$, $a \in \Sigma^+$.

Definition: A Σ-model (W, R, V) is a $(\Sigma, \bar{\cdot})$-model if it respects the converses, i.e. for each $a \in \Sigma$, $R(\overline{a}) = \{(w_1, w_2) \mid (w_2, w_1) \in R(a)\}$.

Regular Languages

A non-deterministic finite automaton (NDFA) $\mathcal{A}$ over alphabet Σ is represented by a quadruple (Q, s, F, δ), where

- Q is a finite set of states,
- $s \in Q$ is the initial state,
- $F \subseteq Q$ is the set of accepting states,
- $\delta \subseteq Q \times \Sigma \times Q$ is the transition relation.

The relation δ can be extended to a relation $\delta^* \subseteq Q \times \Sigma^* \times Q$, which is the smallest relation satisfying:

- for all $a \in \Sigma, \quad q \in Q, \quad (q, a, q) \in \delta^*$,
- for all $a \in \Sigma, \quad u \in \Sigma^*, \quad$ if $(q_1, a, q_2) \in \delta$ and $(q_2, u, q_3) \in \delta^*$, then $(q_1, (a \cdot u), q_3) \in \delta^*$.

An NDFA $\mathcal{A} = (Q, s, F, \delta)$, accepts a word $u \in \Sigma^*$ iff there is an $f \in F$, s.t. $(s, u, f) \in \delta^*$,

For some alphabet Σ, a language L over Σ is a subset $u \subseteq \Sigma^*$.

A language L is regular if there is an NDFA $\mathcal{A}$, s.t.

$$u \in L \text{ iff } \mathcal{A} \text{ accepts } u.$$

A modal logic $\mathcal{L}$ is a regular grammar logic with converse over alphabet Σ iff there is a context-free semi-Thue system S, s.t.

1. each $L_S(a)$ is regular,
2. For a $(\Sigma, \bar{\cdot})$-model $\mathcal{M}$ holds: $\mathcal{M} = (W, R, V)$ is allowed by logic $\mathcal{L}$ iff $\mathcal{M}$ satisfies S.

Standard Modal Logics and their semi-Thue Systems

logic	$\mathrm{L}_{\mathrm{S}}(a)$	frame condition
K	$\{a\}$	(none)
KT	$\{a, \epsilon\}$	reflexivity
KB	$\{a, \overline{a}\}$	symmetry
KTB	$\{a, \overline{a}, \epsilon\}$	refl. and sym.
K4	$\{a\} \cdot \{a\}^*$	transitivity
KT4 = S4	$\{a\}^*$	refl. and trans.
KB4	$\{a, \overline{a}\} \cdot \{a, \overline{a}\}^*$	sym. and trans.
K5	$(\{\overline{a}\} \cdot \{a, \overline{a}\}^* \cdot \{a\}) \cup \{a\}$	euclideanity
KT5 = S5	$\{a, \overline{a}\}^*$	equivalence rel.
K45	$(\{\overline{a}\}^* \cdot \{a\})^*$	trans. and eucl.

Example: For modal logic S4, the language $L_S(a)$ is recognized by the automaton $\mathcal{A} = (Q, s, F, \delta)$, with

- $Q = \{X\}$.
- $s = X$,
- $F = \{X\}$,
- $\delta = \{\ (X, a, X)\ \}$.

Relational Translation for Regular Context-Free Grammar Logics

- For a letter $a \in \Sigma^+$, we define $t_a(\alpha, \beta) = \mathbf{R}_a(\alpha, \beta)$.
- For a letter $a \in \Sigma^-$, we define $t_a(\alpha, \beta) = \mathbf{R}_a(\beta, \alpha)$.

Let $\mathcal{A} = (Q, s, F, \delta)$ be an NDFA. Let $\varphi(\alpha)$ be a *first-order* formula with one free variable α. Assume that for each state $q \in Q$, a fresh unary predicate symbol $\mathbf{q}$ is given. We define $t_{\mathcal{A}}(\alpha, \varphi)$ as the conjunction of the following formulas:

- For the initial state s, add $X_s(\alpha)$,
- for each $q \in Q$, for each $a \in \Sigma$, for each $r \in \delta(q, a)$, add

$$\forall \alpha\beta \; [\; t_a(\alpha, \beta) \to X_q(\alpha) \to X_r(\beta) \;],$$

- for each $q \in Q$, for each $r \in \delta(q, \epsilon)$, add the formula

$$\forall \alpha \; [\; X_q(\alpha) \to X_r(\alpha) \;],$$

- for each $q \in F$, add the formula

$$\forall \alpha \; [\; X_q(\alpha) \to \varphi(\alpha) \;].$$

Relational Translation for Regular Grammar Logics

- $t(p, \alpha, \beta)$ equals $\mathbf{P}(\alpha)$,
- $t(\neg p, \alpha, \beta)$ equals $\neg\mathbf{P}(\alpha)$,
- $t(\psi_1 \wedge \psi_2, \alpha, \beta)$ equals $t(\psi_1, \alpha, \beta) \wedge t(\psi_2, \alpha, \beta)$,
- $t(\psi_1 \vee \psi_2, \alpha, \beta)$ equals $t(\psi_1, \alpha, \beta) \vee t(\psi_2, \alpha, \beta)$,
- for $a \in \Sigma$, $t(\langle a \rangle\ \psi,\ \alpha, \beta)$ equals $\exists\beta\ [\ t_a(\alpha, \beta) \wedge t(\psi, \beta, \alpha)\ ]$,
- for $a \in \Sigma$, $t([a]\ \psi,\ \alpha, \beta)$ equals $t_{\mathcal{A}_a}(\alpha, t(\psi, \alpha, \beta)\ )$.

Theorem:

Let S be a regular semi-Thue system. Let φ be a modal formula. Then φ is satisfiable in a $(\Sigma, \bar{\cdot})$-model satisfying S iff $t(\psi, \alpha, \beta)$ is first-order satisfiable, where $t(\psi, \alpha, \beta)$ is the relational translation for regular grammar logics, based on the automata $\mathcal{A}_a$, for $a \in \Sigma$.

Characterizing the Borders of the Method

One would like to find a logic for which the method does not work, and is unlikely to work.

Idea: Construct a non-regular semi-Thue system S.

This is easy: For example consider $S = \{a \to \overline{a}\overline{a}a\}$.

Problem:

There may exist different semi-Thue systems for the same logic $\mathcal{L}$.

Some other system S', may characterize by the same set of $(\Sigma, \bar{\cdot})$-models but be regular.

Generally, one can add rules, induced by cycles, without changing the set of $(\sigma, \bar{\cdot})$-frames.

Example: For example $S' = \{a \to \overline{a}\overline{a}a, \quad a \to \overline{a}aa\}$.

In fact, very many nodes become connected in larger models, and there probably is a trivial S'' characterizing $\mathcal{L}_S$.

Let Σ be an alphabet. We define the expansion system E_Σ of Σ as

$$\{u \cdot \overline{u} \cdot u \rightarrow u \mid u \in \Sigma^+\}.$$

Theorem Let Σ be a semi-Thue system, which is closed under converse, then for all strings $u, v \in \Sigma^*$,

$$u \Rightarrow^*_{S \cup E_\Sigma} v$$

iff in every $(\sigma, \bar{\cdot})$-model satisfying S, $\quad R_v \subseteq R_u$.

Proof (very very sketchy)

The proof from left to right is more or less trivial.

From right to left: Assume in every $(\sigma, \bar{\cdot})$-model satisfying S, one has $R_v \subseteq R_u$.

Let $M_v = (W, R)$ be a frame consisting of a single path, labeled with v. Call its starting point w_s, and its end point w_e.

Let $M'_v = (W, R')$ be the smallest frame which contains M_v, and which is a $(\sigma, \bar{\cdot})$-model.

It must be the case that $(w_s, w_e) \in R'(u)$.

There exists a word z, wich corresponds to a walk from w_s to w_e in M_v, s.t. $u \Rightarrow_S^* z$.

It remains to show that $z \Rightarrow_{E_\Sigma}^* v$, which can be shown by induction on the number of reverses.

Conclusions, Future Work, Open Problems

- We gave a simple, logspace translation from regular grammar logics with converse to an EXPTIME-complete fragment of first-order logic.
- It would be interesting to implement the translation and to compare it to other decision procedures.
- (Understand better what the border of the translation is. Is there a case where regularity on graphs is not the same as regularity on strings?)