Modal specifications are a syntactic fragment of the Mu-calculus

Guillaume Feuillade

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Modal specifications are a syntactic fragment of the Mu-calculus

Guillaume Feuillade

N° 5612

Juillet 2005

Thème COM

ISSN 0249-6399 ISRN INRIA/RR--5612--FR+ENG

Modal specifications are a syntactic fragment of the Mu-calculus

Guillaume Feuillade*

Thème COM — Systèmes communicants
Projet S4

Rapport de recherche n° 5612 — Juillet 2005 — 17 pages

Abstract: In this report we introduce modal specifications, a new object dedicated to specify some branching-time properties for systems. Modal specifications are a useful tool for studying Petri net synthesis although this aspect is not presented here. The main purpose of this report is to establish the equivalence between a syntactic fragment of the Mu-calculus, namely the conjunctive Nu-calculus and modal specifications. We give the algorithm for constructing a conjunctive Nu-calculus sentence equivalent to a modal specification and the converse. We also study the structure of the set of models of a modal specification.

Key-words: Mu-calculus, rational languages, specification

* INRIA Rennes, projet S4

Spécifications modales : un fragment syntaxique du Mu-calcul

Résumé : Ce document introduit un nouvel objet dédié à la spécification, pour un système, de propriétés du temps arborescent : les spécifications modales. Les spécifications modales sont un outil utilisé pour l'étude de la synthèse de réseaux de Petri ; cet aspect n'étant toutefois pas abordé ici. Le principal objectif de ce rapport est d'établir l'équivalence d'expressivité entre un fragment syntaxique du Mu-calcul (le Nu-calcul conjonctif) et les spécifications modales. Nous donnons l'algorithme permettant la construction d'une spécification modale équivalente à une sentence du Mu-calcul et réciproquement. Nous étudions également la structure formée par l'ensemble des modèles d'une spécification modale.

Mots-clés : Mu-calcul, langages rationnels, spécification

1 Introduction

Branching time logics are a powerful tool for specifying system properties; they are widely used in the areas of verification and control. Most of these logics are subsumed by the Mu-calculus which is a fix-point-based branching time logic. In our work, we consider Mu-calculus as a basis in order to look at decidable logical fragment for Petri net synthesis. As a consequence, we define a syntactic fragment of the Mu-calculus, called the conjunctive modal Nu-calculus, which is well-suited for studying decidability bounds for Petri net synthesis. However, the conjunctive modal Nu-calculus leads to complex proofs in the field of Petri nets. Since we want a more language-based approach to branching-time properties that can be expressed using this logic, we introduce modal specifications. Since these specification are designed as tuple of rational languages, it is easier to establish links between Petri net synthesis for rational languages and Petri net synthesis for modal specifications than for conjunctive modal Nu-calculus. In this report, we prove that conjunctive modal Nu-calculus and modal specifications have the same expressive power and that we can switch between both without loss of generality. We also prove that the set of models of a modal specification is a lattice with finite models as extrema.
The report is organized as follows: first, in section II, we define the modal Mu-calculus from which we extract the conjunctive modal Nu-calculus as a syntactic fragment; then, in section III, we present modal specifications and we prove that the set of models is a lattice; and finally section IV is dedicated to the proof of the equivalence between modal specifications and modal Nu-Calculus.

1.1 Some definitions

Let $\Sigma = \{a_1, \dots a_n\}$ be a finite alphabet. We consider the languages over Σ, with $L, R \dots$ as typical elements and with the usual notations: L^*, $L.a$ with $a \in \Sigma$, etc. The empty word is noted 1. When u and v are two elements of Σ^*, $u.v$ designate the concatenation of u and v and $u^* = \{u^k \mid k \in \mathbb{N}\}$ where u^k is the concatenation of k times the word u.

Definition 1.1. Let L be a language, we say that L is *prefix-closed* if and only if $1 \in L$ and for all word $a_1 \dots . a_m \in L$ we have $a_1 \dots . a_{m-1} \in L$. The prefix-closure of a language L is the least prefix-closed language which is a superset of L. We note $L_{/w} = \{v \in \Sigma^* \mid w.v \in L\}$ the *set of suffixes* of w in L.

Let us remark that the empty language is not prefix-closed by definition, we will have to treat it separately when needed; in particular, for a prefix-closed language L, the language $L_{/w}$ is either prefix-closed -if $w \in L$- or empty. In the following, L always denotes a prefix-closed language.

2 Modal mu-calculus and conjunctive modal nu-calculus

In this section we give the definition of modal mu-calculus formulas and of a syntactic fragment of the modal mu-calculus - the conjunctive nu-calculus -. We also provide an interpretation of formulas over prefix-closed languages instead of the one over processes given for example in [AN01]. These two interpretations are the same with the convention that a language denotes the set of states of a process which can be reach by following the transition sequence of each word of the language. However, the language presentation given here brings more readable proofs.

2.1 mu-calculus over prefix-closed languages

We give the definition of modal mu-calculus formulas and an interpretation over prefix-closed formulas. Let $Var = \{X, X_1, X_2, \dots\}$ be a set of variables.

Definition 2.1. (Syntax of the Mu-calculus)
The set of modal mu-calculus formulas is noted L_μ and is defined by the following grammar:

$$(L_\mu \ni) \quad \beta_1, \beta_2 ::= \texttt{true} \mid X \mid \ <a> \beta_1 \mid \neg\beta_1 \mid \beta_1 \vee \beta_2 \mid \mu X.\beta_1(X)$$

where $a \in \Sigma$ and with the requirement that all variable X is under the scope of an even number of negation symbols $\neg$ in $\beta_1(X)$ for all formula $\mu X.\beta_1(X)$ -in order to ensure the existence of fixed-points-.

We note $\texttt{false}, [a]\beta_1, \beta_1 \wedge \beta_2, \rightarrow^a, \not\rightarrow^a$ and $\nu X.\beta_1(X)$ the respective formulas $\neg\texttt{true}, \neg <a> (\neg\beta_1), \neg(\neg\beta_1 \vee \neg\beta_2), <a>\texttt{true}, [a]\texttt{false}$ and $\neg\mu X.\neg\beta_1(\neg X)$.

We say that the X-variable is *free in* β if it is not under the scope of any $\mu.X$ or $\nu.X$ operator. The set of free variables in β is noted $var(\beta)$. A formula β without any free variable is called a *sentence*.

We define an interpretation of modal mu-calculus formulas over prefix-closed languages over the alphabet Σ. The interpretation of a mu-calculus formula over a prefix-closed language L is the set of words of L satisfying the formula according to a given interpretation *val* over the free variables of the formula; this set is not necessarily prefix-closed.

Definition 2.2. (Semantic of L_μ over prefix-closed languages)
the interpretation over a prefix-closed language $L \subseteq \Sigma^*$ of a sentence $\beta \in L_\mu$ according to a valuation $val : Var \to L$ is the set $[\![\alpha]\!]_L^{[val]} \subseteq L$ which is inductively defined by:

$$\begin{aligned}
&[\![\texttt{true}]\!]_L^{[val]} = L \\
&[\![X]\!]_L^{[val]} = val(X) \\
&[\![\neg\alpha]\!]_L^{[val]} = L \setminus [\![\alpha]\!]_L^{[val]} \\
&[\![\beta_1 \vee \beta_2]\!]_L^{[val]} = [\![\beta_1]\!]_L^{[val]} \cup [\![\beta_2]\!]_L^{[val]} \\
&[\![<a> \beta_1]\!]_L^{[val]} = \{w \in L \mid w.a \in [\![\beta_1]\!]_L^{[val]}\} \\
&[\![\mu X.\beta_1(X)]\!]_L^{[val]} = \bigcap\{V \subseteq L \mid [\![\beta_1]\!]_L^{[val(V/X)]} \subseteq V\}
\end{aligned}$$

where the valuation $val(V/X) : Var \rightarrow \mathcal{P}(L)$ is given by $val(V/X)(X') = V(X')$ for all variable $X' \in Var$ such that $X' \neq X$ and $val(V/X)(X) = V$.

The interpretation $[\![\mu X.\beta(X)]\!]_L^{[val]}$ (resp. $[\![\nu X.\beta(X)]\!]_L^{[val]}$) is the least fixed-point (resp. greatest fixed-point) of the function $V \mapsto [\![\beta]\!]_L^{[val(V/X)]}$. The semantic of mu-calculus sentences does not depend on the valuation; in this case, we note $[\![\beta]\!]_L$ the interpretation of β according to any valuation. We say that "the language L *satisfies* the sentence β" -$L \models \beta$ for short- if and only if $1 \in [\![\beta]\!]_L$.

2.2 Conjunctive nu-calculus

We extract a syntactic fragment of L_μ. This fragment will be our basis for a new language-based representation which is the main purpose of this report.

Definition 2.3. (Conjunctive modal Nu-calculus)
The set of nu-calculus formulas is noted L_ν and is the fragment of L_μ defined by the following restriction of the grammar of L_μ with $a \in \Sigma$:

$$(L_\nu \ni) \quad \beta_1, \beta_2 ::= \texttt{true} \mid X \mid \rightarrow^a \mid [a]\beta_1 \mid \not\rightarrow^a \mid \beta_1 \wedge \beta_2 \mid \nu X.\beta_1(X)$$

The interpretation of a formula $\beta \in L_\nu$ over a prefix-closed language $L \subseteq \Sigma^*$ according to a valuation $val : Var \rightarrow L$ is given by the semantic of the same formula in L_μ; that is :

$$\begin{array}{l}
[\![\texttt{true}]\!]_L^{[val]} = L \\
[\![X]\!]_L^{[val]} = val(X) \\
[\![\rightarrow^a \beta]\!]_L^{[val]} = \{w \in L \mid w.a \in L\} \\
[\![\not\rightarrow^a]\!]_L^{[val]} = \{w \in L \mid w.a \notin L\} \\
[\![[a]\beta]\!]_L^{[val]} = \{w \in L \mid w.a \in [\![\beta]\!]_L^{[val]}\} \cup \{w \in L \mid w.a \notin L\} \\
[\![\beta_1 \wedge \beta_2]\!]_L^{[val]} = [\![\beta_1]\!]_L^{[val]} \cap [\![\beta_2]\!]_L^{[val]} \\
[\![\nu X.\beta(X)]\!]_L^{[val]} = \bigcup \{V \subseteq L \mid [\![\beta]\!]_L^{[val(V/X)]} \supseteq V\}
\end{array}$$

The operator $<a>\ \beta$ of L_μ can be expressed by $[a]\beta \wedge \rightarrow^a$ in L_ν. However, the following operators cannot be expressed in L_ν : $\beta_1 \vee \beta_2$, $\mu X.\beta(X)$, $\texttt{false}$. The disjunctive operator $\vee$ is now only implicitly present in the operator $[a]\beta$ which could be expressed by $<a>\ \beta \vee \not\rightarrow^a$ in L_μ.

3 Modal specifications and its models

In this section, we propose a new mean for specifying a set of models, namely modal specifications. We show in the next section that modal specifications are strictly equivalent to conjunctive nu-calculus sentences. However, the fist goal of modal specifications is to

ease the analysis of the set of models of a sentence of L_ν, while the second goal, which is not presented in this report, is to permit the extraction of a structural fragment for which unlabeled Petri net synthesis is decidable.

3.1 Definitions

Definition 3.1. (Modal specification)
A modal specification is a tuple $S = \langle \{C_a\}_{a\in\Sigma}, I\rangle$ where, for all $a \in \Sigma$, C_a is a rational language of words that *must* enable an action a and I is the rational language of forbidden words. The *completion operator* associated to S, noted C_S is the application $C_S : \mathcal{P}(\Sigma^*) \to \mathcal{P}(\Sigma^*)$ defined by : $C_S(L) = \bigcup_{a\in\Sigma}(L \cap C_a).a$.

A modal specification defines a set of models which are prefix-closed languages. We define the semantic of a modal specification as a set of models in the following way:

$$mod(S) = \{L \subseteq \Sigma^* \mid C_S(L) \subseteq L \wedge L \cap I = \emptyset\}$$

From this definition, we say that S is *satisfiable* if $mod(S) \neq \emptyset$ and that L *satisfies* S if $L \in mod(S)$. The models of S are then the languages satisfying the following two conditions:

- for each word w of L in C_a, $w.a$ must be a word of L,
- no word of L may be in I.

Remark that the models of a modal specification may not be rational languages. However, as modal specifications are designed to be equivalent to a fragment of the mu-calculus, they inherit the *finite model property* as we will show latter and then, when $mod(S)$ is nonempty, S has a rational model.

3.1.1 Graphical representation

In order to be able to give visual examples, we define a graphical representation of modal specifications: modal automata. These automata put together all the components of modal specification. A modal automaton is an automaton without final states where each arc is either a plain line or a dotted line.

Let $\Sigma = \{a, b, c\}$. We note $\mathcal{L}(q)$ the language of the automaton with q as a final state and where each transition is considered as a *normal* transition *i.e* replacing the dotted lines by plain lines to get an usual automaton. In figure 1 $\mathcal{L}(q_1) = (a^*b^+)^*$ and $\mathcal{L}(q_2) = (a^*b^+)^*a$.

- a continuous arc issuing a state q and labeled by a means that the transition a *must* be performed by the system from state q
- a dotted arc issuing a state q and labeled by a means that the transition a *is allowed* to the system from state q

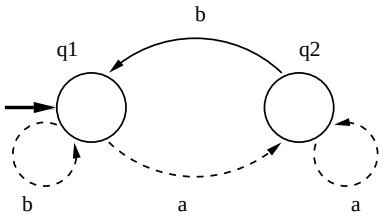

Figure 1: a modal automaton

- no a-labeled arc issuing a state q means that the transition a is forbidden from this state

These three informal rules can be reformulated in terms of modal specification. Let $S = \langle \{C_a\}_{a\in\Sigma}, I\rangle$ be the modal specification associated with the automaton, the three rules becomes :

- a continuous arc issuing a state q and labeled by a stands for $\mathcal{L}(q) \subseteq C_a$
- a dotted arc issuing a state q and labeled by a stands only for the structure
- no a-labeled arc issuing a state q stands for $\mathcal{L}(q).a \in I$

Example 3.2. *The automaton of the figure 1 represent the modal specification* $S = \langle \{C_a\}_{a\in\Sigma}, I\rangle$ *with* $C_a = \emptyset$, $C_b = (a^*b)^*a$, $C_c = \emptyset$ *and* $I = \Sigma^*.c$.

3.1.2 Coherency and S-closure

We say that a specification $S = \langle \{C_a\}_{a\in\Sigma}, I\rangle$ is *coherent* if 'S is satisfiable' implies $I \cap C_S(\Sigma^*) = \emptyset$. For a satisfiable modal specification, being coherent corresponds to requiring that from every word w, no action a is both imposed by S ($w \in C_a$) and forbidden by S ($w.a \in I$).

Lemma 3.3. *Every modal specification is equivalent model-wise to a coherent modal specification.*

Proof. From a satisfiable modal specification $S = \langle \{C_a\}_{a\in\Sigma}, I\rangle$, we construct the modal specification $S' = \langle \{C'_a\}_{a\in\Sigma}, I\rangle$ such that for all $a \in \Sigma$, $C'_a = C_a \setminus \{w \in \Sigma^* \mid w.a \in I\}$. By construction $I \cap C_S(\Sigma^*) = \emptyset$, hence S' is coherent. It is obvious that $mod(S) = mod(S')$. □

From this point we consider only coherent modal specifications. Suppose a language L verifies $L \cap I = \emptyset$ but not $C_S(L) \subseteq L$, it is often possible to "complete" L in order to obtain a model of S.

Definition 3.4. (S-closure)
The S-closure of a prefix-closed language L, noted $L{\uparrow}^S$, is the least language L' such that $L \subseteq L'$ and $L' \in mod(S)$.

Lemma 3.5. *The S-closure of a rational language is rational*

Proof. We show this property by building a finite automaton recognizing the S-closure of a given prefix-closed rational language L:

1. build the automaton $\mathcal{A}$ recognizing $L \cup \bigcup_{a\in\Sigma} C_a.a$,
2. remove from $\mathcal{A}$ all the non-terminal states. This gives a new automaton $\mathcal{A}'$ recognizing the greatest prefix-closed language included in $L \cup \bigcup_{a\in\Sigma} C_a.a$,
3. return $\mathcal{L}(\mathcal{A})$.

Since L is prefix-closed, then $L \subseteq \mathcal{L}(\mathcal{A}')$ and obviously $L{\uparrow}^S \subseteq \mathcal{L}(\mathcal{A}')$; moreover if $L{\uparrow}^S \subsetneq \mathcal{L}(\mathcal{A}')$ then, since $L{\uparrow}^S$ and $\mathcal{L}(\mathcal{A}')$ are prefix-closed, there exist $w \in L{\uparrow}^S$ and $a \in \Sigma$ such that $w.a \in \mathcal{L}(\mathcal{A}')$ and $w.a \notin L{\uparrow}^S$, thus $w \in C_a$, which contradict $L{\uparrow}^S \in mod(S)$. □

The following lemma gives another definition to the S-closure equivalent to the previous one.

Lemma 3.6. *The S-closure of a prefix-closed language L is the least solution of the equation $R = L \cup C_S(R)$.*

Proof. By definition $L{\uparrow}^S \in mod(S)$, then $C_S(L{\uparrow}^S) \subseteq L{\uparrow}^S$. Since $L \subseteq L{\uparrow}^S$, we get $L \cup C_S(L{\uparrow}^S) \subseteq L{\uparrow}^S$. From $L{\uparrow}^S$ being the least language we get the equality $L{\uparrow}^S = L \cup C_S(L{\uparrow}^S)$. □

Example 3.7. *Let S be the modal specification of figure 1, let $L = (a^*)$. The S-closure of L is $L{\uparrow}^S = (a^* \cup a^*.b)$.*

3.2 Set of models of a modal specification

We show in this part how to construct the two trivial models of a satisfiable modal specification and that the set of models of a modal specification forms a lattice which extrema are these two trivial models.

We fix $S = \langle \{C_a\}_{a\in\Sigma}, I\rangle$ a coherent modal specification. We note $L^S_\perp$ for $\{1\}{\uparrow}^S$ and $L^S_\top$ for $\Sigma^* \setminus I.\Sigma^*$.

Lemma 3.8. *These four propositions are equivalent :*

1. *S is satisfiable*
2. *$L^S_\perp \in mod(S)$*
3. *$L^S_\perp \cap I = \emptyset$*

4. $L^S_\top \in mod(S)$

Proof. Since $2 \Rightarrow 1$, $4 \Rightarrow 1$ et $2 \Rightarrow 3$ are trivial, we show $3 \Rightarrow 2$, $1 \Rightarrow 4$ and $4 \Rightarrow 3$.

- $3 \Rightarrow 2$: by lemma 3.6 we get $L^S_\bot = \{1\} \cup C_S(L^S_\bot)$, then $C_S(L^S_\bot) \subseteq L^S_\bot$ and by hypothesis $L^S_\bot \cap I = \emptyset$, thus $L^S_\bot \in mod(S)$;
- $1 \Rightarrow 4$: S is coherent, meaning $C_S(\Sigma^*) \cap I = \emptyset$ holds, and $C_S(L^S_\top) \subseteq C_S(\Sigma^*)$, then $C_S(L^S_\top) \subseteq L^S_\top$ and $L^S_\top \cap I = \emptyset$, finally $L^S_\top \in mod(S)$;
- $4 \Rightarrow 3$: $L^S_\top \cup C_S(L^S_\top) = L^S_\top$ then $L^S_\bot \subseteq \{1\} \cup C_S(L^S_\top) \subseteq L^S_\top$ and $L^S_\top \cap I = \emptyset$; we get $L^S_\bot \cap I = \emptyset$.

□

From this lemma, we retrieve the equivalent of the *finite model property* of L_μ: if S is satisfiable then it has a rational model ($L^S_\bot$ is rational by lemma 3.5 and $L^S_\top$ is rational by definition). In the case of modal specification, these rational models are, by construction, the extrema of the models of S ordered by inclusion : $L^S_\top$ is the greatest model and $L^S_\bot$ is the least one.

Theorem 3.9. *If S is satisfiable then $(mod(S), \subseteq)$ is a distributive complete lattice.*

Proof. By definition of $mod(S)$. □

Example 3.10. *Let S be the modal specification of figure 2. Some of the models of S are depicted in figure 3; the boxes represent the models and the arrows between boxes represent the language inclusion relation. Clearly $L_\top = L7$ and $L_\bot = L1$. There exists an infinite number of models between $L2$ and $L4$ as between $L3$ and $L5$ or $L4$ and $L7$. The model $L6$ shows that $L4 \cup L5 \neq L7$.*

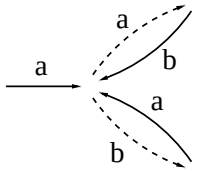

Figure 2: The modal specification S

3.3 A compositional approach to modal specifications

We now give a compositional approach for modal specifications. We show that each modal specification can be expressed as a composition of simple modal specifications with a set of operators. Then in the following section, we use this expression in order to prove the model equivalence with L_ν. First we give the operators.

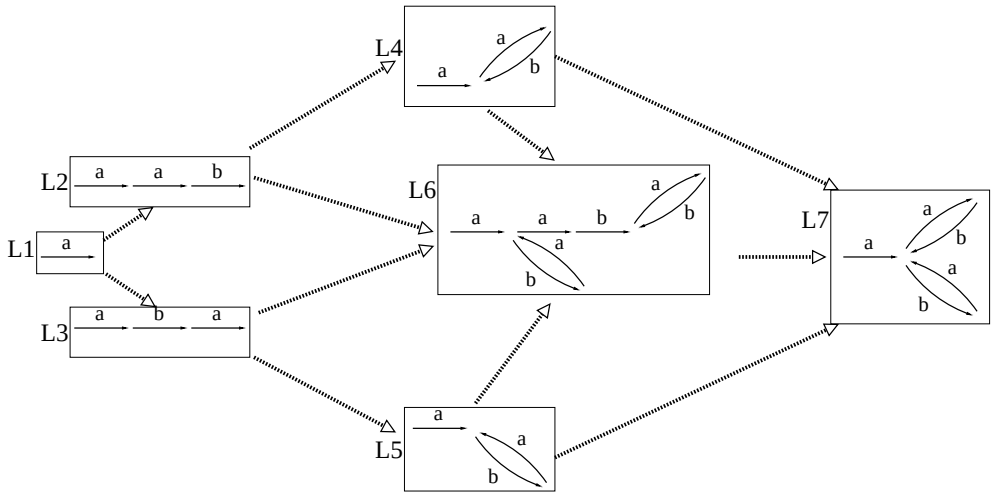

Figure 3: Some elements of the lattice of models of S

3.3.1 Atomic specifications and operators

Definition 3.11. Let $S_1 = \langle \{C_a^1\}_{a\in\Sigma}, I^1\rangle$ and $S_2 = \langle \{C_a^2\}_{a\in\Sigma}, I^2\rangle$

- The *intersection* of two specifications $S_1 = \langle \{C_a^1\}_{a\in\Sigma}, I^1\rangle$ and $S_2 = \langle \{C_a^2\}_{a\in\Sigma}, I^2\rangle$, is the specification $S_1 \cap S_2 = \langle \{C_a^1 \cup C_a^2\}_{a\in\Sigma}, I^1 \cup I^2\}\rangle$.
- The *prefixing* of a specification S_1 by a language $R \subseteq \Sigma^*$ is the specification $R.S_1 = \langle \{R.C_a\}_{a\in\Sigma}, R.I\rangle$.

The intersection of two specification corresponds to the 'and': a language is model of the intersection if and only if it is model of the two specifications.

Lemma 3.12. *Let S_1 and S_2 be two modal specifications, $mod(S_1 \cap S_2) = mod(S_1) \cap mod(S_2)$.*

Proof. For all $L \in mod(S_1 \cap S_2)$, we have $C_{S_1\cap S_2}(L) \subseteq L$ and $C_{S_1\cap S_2}(L) = C_{S_1}(L) \cup C_{S_2}(L)$, thus $C_{S_1}(L) \subseteq L$ and $C_{S_2}(L) \subseteq L$. Moreover $(I_1 \cup I_2) \cap L = \emptyset$, then $I_1 \cap L = I_2 \cap L = \emptyset$, thus $L \in mod(S_1) \cap mod(S_2)$. Reciprocally, $L \in mod(S_1) \cap mod(S_2)$ implies $C_{S_1}(L) \cup C_{S_2}(L) \subseteq L$ and $I_1 \cap L = I_2 \cap L = \emptyset$; finally $L \in mod(S_1 \cap S_2)$. □

The prefixing of a specification S by a language R is the specification which is satisfied exactly by the languages for which each suffix language of a word in R satisfies the specification S.

Lemma 3.13. *For all* $L \subseteq \Sigma^*$,

$$L \in mod(R.S) \Leftrightarrow \forall w \in R, L_{/w} = \emptyset \text{ or } L_{/w} \in mod(S)$$

where $L_{/w}$ *is the set of suffixes of* w *in* L.

Proof. For this proof, the fact that $L \cap v.\Sigma^* = v.L_{/v}$ then $L \cap v.L' = v.(L_{/v} \cap L')$ and also $w.L_1 \subseteq L_2 \Rightarrow L_1 \subseteq L_{2/w}$ is used several times without mentioning it.

$\Rightarrow$) Let $L \in mod(R.S)$, by the construction of $R.S$:

$$C_{R.S}(L) = \bigcup_{a\in\Sigma} (L \cap R.C_a).a = \bigcup_{a\in\Sigma} \bigcup_{w\in R} (L \cap w.C_a).a = \bigcup_{a\in\Sigma} \bigcup_{w\in R} w.(L_{/w} \cap C_a).a$$

Since $C_{R.S}(L) \subseteq L$, for all $w \in R$ and for all $a \in \Sigma^*$, $w.(L_{/w} \cap C_a).a \subseteq L$, then $C_s(L_{/w}) \subseteq L_{/w}$. Similarly, since $L \cap R.I = \emptyset$, we get for all $w \in R$, $L \cap w.I = \emptyset$ and then $L_{/w} \cap I = \emptyset$. Finally $L_{/w} = \emptyset$ or $L_{/w} \in mod(S)$.

$\Leftarrow$) We show first that for all $a \in \Sigma$, $(L \cap R.C_a).a \subseteq L$. Let $v \in L \cap R.C_a$, there exist $w \in R$ and $u \in C_a$ such that $v = wu$. Then $u \in L_{/w} \cap C_a$ with $L_{/w} \neq \emptyset$. By hypothesis, $L_{/w} \in mod(S)$, then $(L_{/w} \cap C_a).a \subseteq L_{/w}$ and in particular $u.a \in L_{/w}$. We deduce $v.a = w.u.a \in L$. We show now that $L \cap R.I = \emptyset$: for all $w \in R$, if $L_{/w} = \emptyset$ then $L \cap w.I = \emptyset$; otherwise $L_{/w} \in mod(S)$ then $L \cap w.I = \emptyset$; finally $L \cap R.I = \emptyset$. □

Definition 3.14. We define the following set of atomic specifications:
$S_{\mathtt{true}} = \langle \{\emptyset\}_{a\in\Sigma}, \emptyset \rangle$,
$S_{\not\rightarrow b} = \langle \{\emptyset\}_{a\in\Sigma}, \{b\} \rangle$ and
$S_{\rightarrow b} = \langle \{C_a\}_{a\in\Sigma}, \emptyset \rangle$, with $C_a = \emptyset$ for $a \neq b$ and $C_b = \{1\}$.

The sets of models of the atomic specifications are then obtained by definition and are:

$$\begin{array}{lcl} mod(S_{\mathtt{true}}) & = & \{L \in \Sigma^*\} \\ mod(S_{\not\rightarrow_b}) & = & \{L \subseteq \Sigma^* \mid b \notin L\} \\ mod(S_{\rightarrow_b}) & = & \{L \subseteq \Sigma^* \mid b \in L\} \end{array}$$

3.3.2 Compositional approach

Theorem 3.15. *Each modal specification can be expressed as a composition of atomic ones with the union and the language-prefixing operators*

Proof. Let $S = \langle \{C_a\}_{a\in\Sigma}, I \rangle$ be a modal specification, for a in Σ we define the set $I^a = \{u \in \Sigma^* \mid u.a \in I\}$. Let $S' = \langle \{C'_a\}_{a\in\Sigma}, I' \rangle$ be the specification defined by

$$S' = \bigcup_{a\in\Sigma} C_a.S_{\rightarrow a} \cup \bigcup_{a\in\Sigma} I^a.S_{\not\rightarrow a}$$

By definition 3.11 and 3.14, it is obvious that $S = S'$. □

4 Conjunctive modal nu-calculus and modal specifications are equivalent

This section is dedicated to the proof of the following theorem:

Theorem 4.1. *For all set E of prefix-closed languages, E is the set of models of a sentence β of L_ν if and only if there exists a modal specification S such that $E = mod(S)$.*

In order to prove this theorem, we introduce the notion of variable paths:

Definition 4.2. (variable paths)
Let β be a formula of L_ν, we define an application $P_\beta : var(\beta) \to \mathcal{P}(\Sigma^*)$, by induction over the structure of β:
for all $X \in var(\beta)$,

- $\beta \in \{\mathtt{true}, \to^a, \not\to^a\}$, then $P_\beta(X) = \emptyset$,
- $\beta = Y$ and $Y \neq X$, then $P_\beta(X) = \emptyset$,
- $\beta = X$, then $P_\beta(X) = \{1\}$,
- $\beta = [a]\alpha$, then $P_\beta(X) = a.P_\alpha(X)$,
- $\beta = \beta_1 \wedge \beta_2$, then $P_\beta(X) = P_{\beta_1}(X) \cup P_{\beta_2}(X)$,
- $\beta = \nu Y.\alpha(Y)$, then $P_\beta(X) = P_\alpha(Y)^*.P_\alpha(X)$.

The language $P_\beta(X)$ is the set of *variable paths* of X in β.

Example 4.3. *Some examples of variable-paths:*

- *if $\beta = [a]X$, then $P_\beta(X) = \{a\}$,*
- *if $\beta = [a][b]X \wedge [c]X$, then $P_\beta(X) = (a.b + c)$,*
- *if $\beta = \nu Y.([a][b]Y \wedge [c]X)$, then $P_\beta(X) = (a.b)^*.c$*

The variable paths of X are the words that 'lead' to an occurrence of X in the formula: when $w \in [\![\beta]\!]_L^{[val]}$, $P_\beta(X)$ is the set of words v such that $w.v \in [\![X]\!]_L^{[val]}$ or equivalently $w.v \in val(X) \subseteq L$.

4.1 From a sentence to a specification

We show here how to construct a modal specification S_β from a sentence β of L_ν such that $mod(S_\beta)$ is the set of models of β. This is a constructive proof for the implication of theorem 4.1: E is the set of models of a sentence of L_ν implies the existence of S such that $mod(S) = E$.
This proof is achieved by induction over the sentence β. Consequently, we need to prove it

for all *formula* of L_ν. Since modal specifications are not designed to deal with valuations, we introduce the following hypothesis, related to a valuation val, a formula β, a language L and a word w of L :

$$\forall X \in var(\beta), w.P_\beta(X) \cap L \subseteq val(X) \quad (1)$$

The hypothesis (1) states that the words of L that coincide with words of a variable path, say for a variable X, must be in $val(X)$.

Definition 4.4. (Modal specification associated to a formula of L_ν)
We define the modal specification S_β *associated to the formula* $\beta \in L_\nu$ inductively over the structure of β :

- $\beta \in \{\mathtt{true}, \rightarrow^a, \not\rightarrow^a\}$, S_β is given by definition 3.14,
- $\beta = X$, $S_\beta = S_{\mathtt{true}}$,
- $\beta = [a]\alpha$, $S_\beta = a.S_\alpha$,
- $\beta = \beta_1 \wedge \beta_2$, $S_\beta = S_{\beta_1} \cap S_{\beta_2}$,
- $\beta = \nu Y.\alpha(Y)$, $S_\beta = P_\alpha(Y)^*.S_\alpha$.

Example 4.5. *Let* $\beta = [a]\nu X.([b]X \wedge \rightarrow^a \wedge \not\rightarrow^c)$*, the modal specification associated to* β *is* $(a.b^*).(S_{\rightarrow^a} \cap S_{\not\rightarrow^c})$ *i.e the specification* $S_\beta = \langle \{C_a\}_{a\in\Sigma}, I\rangle$ *with:*

$$C_a = (a.b^*), C_b = \emptyset, C_c = \emptyset, I = (a.b^*)$$

Proposition 4.6. *Let* $\beta \in L_\nu$*, val be a valuation,* L *be a prefix-closed language and* w *be a word of* L*.*

$$w \in [\![\, \beta \,]\!]_L^{[val]} \Leftrightarrow L_{/w} \in mod(S_\beta) \text{ and hypothesis (1) is verified}$$

The first implication of theorem 4.1 appears as a corollary of proposition 4.6:

Corollary 4.7. (of proposition 4.6)
For every sentence β *of* L_ν*,* S_β *and* β *have the same set of models*

Let $\beta \in L_\nu$, val be a valuation, L be a prefix-closed language and w be a word of L. To prove proposition 4.6, we prove these 3 following lemmas:

Lemma 4.8.

$$w \in [\![\, \beta \,]\!]_L^{[val]} \Rightarrow \text{hypothesis (1)}$$

Lemma 4.9.

$$w \in [\![\, \beta \,]\!]_L^{[val]} \Rightarrow L_{/w} \in mod(S_\beta)$$

Lemma 4.10.

$$L_{/w} \in mod(S) \text{ and hypothesis (1)} \Rightarrow w \in [\![\beta]\!]_L^{[var]}$$

Proof. **(of lemma 4.8)**
Let $w \in [\![\beta]\!]_L^{[val]}$. The proof is by induction over the structure of β:

- $\beta \in \{\mathtt{true}, \rightarrow^a, \not\rightarrow^a\}$, $var(\beta) = \emptyset$,
- $\beta = X$, $var(\beta) = \{X\}$, then $P_X(X) = \{1\}$ and $w \in [\![X]\!]_L^{[val]}$, thus $w \in val(X) \Rightarrow w.\{1\} \subseteq valX$
- $\beta = [a]\alpha$, $var(\beta) = var(\alpha)$ and $P_\beta(X) = a.P_\alpha(X)$, then $w.P_\beta(X) \cap L = w.a.P_\alpha(X) \cap L$. Since $w.a \in [\![\alpha]\!]_L^{[val]}$, by induction hypothesis, $w.P_\beta(X) \cap L \subseteq val(X)$,
- $\beta = \beta_1 \wedge \beta_2$, then $w.P_\beta(X) \cap L = (w.P_{\beta_1}(X) \cap L) \cup (w.P_{\beta_1}(X) \cap L)$ and by induction hypothesis, $(w.P_{\beta_1}(X) \cap L) \cup (w.P_{\beta_1}(X) \cap L) \in val(X)$,
- $\beta = \nu Y.\alpha(Y)$, we show by induction on n that:

  $$w.P_\alpha(Y)^n.P_\alpha(X) \cap L \subseteq val(X)$$

  When using induction hypothesis, we precise whether they concern the induction over n or over β.
  Let note $V = [\![\beta]\!]_L^{[val]}$; we have that $w \in [\![\beta]\!]_L^{[val]}$ is equivalent to $w \in [\![\alpha(Y)]\!]_L^{[val(V/Y)]}$.
  - For $n = 0$, by induction hypothesis over β, $w.P_\alpha(X) \cap L \subseteq val(X)$
  - For $n + 1$, $w.P_\alpha(Y)^{n+1}.P_\alpha(X) \cap L = w.P_\alpha(Y).P_\alpha(Y)^n.P_\alpha(X) \cap L$; by induction hypothesis over β, $w \in [\![\alpha(Y)]\!]_L^{[val(V/Y)]}$ then $w.P_\alpha(Y) \cap L \subseteq V$ and then for all $v \in w.P_\alpha(Y) \cap L$, $v \in V$; by induction hypothesis over n, we get $v.P_\alpha(Y)^n.P_\alpha(X) \cap L \subseteq val(X)$ and finally $w.P_\alpha(Y).P_\alpha(Y)^n.P_\alpha(X) \cap L \subseteq val(X)$

□

Proof. **(of lemma 4.9)**
The proof is by induction over the structure of β:

- $\beta \in \{\mathtt{true}, \rightarrow^a, \not\rightarrow^a, X\}$, by definition 3.14, $L_{/w} \in mod(S_\beta)$,
- $\beta = [a]\alpha$, $S_\beta = a.S_\alpha$, if $a \in L_{/w}$ then $w.a \in [\![\alpha]\!]_L^{[val]}$; by induction hypothesis, $L_{/w.a} \in mod(S_\alpha)$. By lemma 3.13, we get $L_{/w} \in mod(S_\beta)$.
- $\beta = \beta_1 \wedge \beta_2$, by lemma 3.12 we get $mod(S_\beta) = mod(S_{\beta_1}) \cap mod(S_{\beta_2})$; then by induction hypothesis, $L_{/w} \in mod(S_\beta)$.
- $\beta = \nu X.\alpha(X)$. Let $V = [\![\beta]\!]_L^{[val]}$, we have $V = [\![\alpha(X)]\!]_L^{val(V/X)}$. We show for all n and for all $v \in (P_{\alpha(X)}(X))^n$, $w.v \in L \Rightarrow L_{/w.v} \in mod(S_\alpha)$ by induction over n.

- For $n = 0$, $w \in [\![\alpha(X)]\!]_L^{val(V/X)}$ and by induction hypothesis over β, $L_{/w} \in mod(S_\alpha)$.
- For $n+1$, $w \in V$ and since $v = u.u'$ with $u \in P_{\alpha(X)}(X)$, by lemma 4.8 we have $(u' \in L_{/w.u}) \Rightarrow L_{/w.u.u'} \in val(X) = V$. It follows by induction hypothesis over n, since $u' \in (P_{\alpha(X)}(X))^n$, that $L_{/w.u.u'} \in mod(S_\alpha)$.

Finally, for all $v \in (P_{\alpha(X)}(X))^*$, $w.v \in L \Rightarrow L_{/w.v} \in mod(S_\alpha)$. We apply lemma 3.13 to get $L_{/w} \in mod(S_\beta)$.

□

Proof. **(of lemma 4.10)**
The proof is by induction over β:

- $\beta \in \{\mathtt{true}, \rightarrow^a, \not\rightarrow^a\ X\}$, by definition 3.14, $w \in [\![\beta]\!]_L^{[var]}$,
- $\beta = [a]\alpha$, $S_\beta = a.S_\alpha$, if $a \in L_{/w}$ then lemma 3.13 ensure $L_{/w.a} \in \mod(S_\alpha)$ and then by induction hypothesis, $w.a \in [\![\alpha]\!]_L^{[val]}$. We have then in both cases $w \in [\![\beta]\!]_L^{[val]}$,
- $\beta = \beta_1 \wedge \beta_2$, $S_\beta = S_{\beta_1} \cup S_{\beta_2}$, by lemma 3.12 we get $L_{/w} \in mod(S_{\beta_1}) \cap mod(S_{\beta_2})$, and by definition 4.2 and by hypothesis (1), for all $v \in P_\beta(X)$, $v \in P_{\beta_1}(X) \cup P_{\beta_2}(X)$. We can now apply induction hypothesis for β_1 and β_2 to get $w \in [\![\beta]\!]_L^{[val]}$,
- $\beta = \nu X.\alpha(X)$, we show that $(L \cap w.P_\alpha(X)^*)$ is a post fix-point:

$$(L \cap w.P_\alpha(X)^*) \subseteq [\![\alpha]\!]_L^{[var(X/(L \cap w.P_\alpha(X)^*)]}$$

For all $v \in (L_{/w} \cap P_\alpha(X)^*)$:

1. $w \in mod(S_\beta) \Rightarrow w.v \in mod(S_\alpha)$ (lemma 3.13),
2. For all $Y \in var(\beta)$ $(Y \neq X)$, $w.P_\beta(Y) \cap L \subseteq val(Y)$ and $P_\beta(Y) = (P_\alpha(X))^* P_\alpha(Y)$ implies
$$w.v.P_\alpha(Y) \cap L \subseteq val(Y)$$
3. For X, $v \in (L_{/w} \cap P_\alpha(X)^*)$ implies
$$w.v.P_\alpha(X) \cap L \subseteq val(X/(L \cap w.P_\alpha(X)^*))$$

The items 2) and 3) gives us hypothesis (1) which together with 1) allows to apply the induction hypothesis in order to obtain $w.v \in [\![\alpha]\!]_L^{[var(X/(L \cap w.P_\alpha(X)^*)]}$. We have proved that $(L \cap w.P_\alpha(X)^*)$ is a post-fixed-point and $w \in (L \cap w.P_\alpha(X)^*)$; we finally get $w \in [\![\beta]\!]_L^{[val]}$.

□

Now the proof of proposition 4.6 is immediate:

Proof. **(of proposition 4.6)**
$\Rightarrow$) is given by lemma 4.10
$\Leftarrow$) is given by lemmas 4.8 and 4.9. □

4.2 From a specification to a sentence

We show here how to construct a formula β_S of L_ν from a modal specification S such that the set of models of β_S is equal to $mod(S)$. This is a constructive proof for the second implication of theorem 4.1. The idea is to express S with atomic specifications according to theorem 3.15 and to construct β_S step by step such that S_{β_S} and S are equal component-wise and then model-wise.

Lemma 4.11. *For all rational language $R \subseteq \Sigma^*$ it is possible to construct a formula $\alpha_R(X) \in L_\nu$ such that for all sentence β of L_ν, $S_{\alpha_R(\beta/X)} = R.S_\beta$.*

Proof. Since R is a rational language, it can be expressed as a regular expression over Σ. In order to proceed inductively, we give a well-chosen grammar generating regular languages

$$\{1\} \mid a.R_1 \mid R_1 \cup R_2 \mid R_1^*$$

where $a \in \Sigma$. We construct inductively $\alpha_R(X)$ and we prove at each step that for all $\beta \in L_\nu$, $S_{\alpha_R(\beta/X)} = R.S_\beta$ and $P_{\alpha_R(X)}(X) = R$:

- $R = \{1\}$: let $\alpha_R(X) = X$, we trivially have $S_{\alpha_R(\beta/X)} = R.S_\beta$ and $P_{\alpha_R(X)}(X) = R$,
- $R = a.R_1$: let $\alpha_R(X) = [a]\alpha_{R_1}(X)$, from definition 4.4 we have $S_{\alpha_R(\beta/X)} = R.S_\beta$, and from definition 4.2 we have $P_{\alpha_R(X)}(X) = R$,
- $R = R_1 \cup R_2$: let $\alpha_R(X) = \alpha_{R_1}(X) \wedge \alpha_{R_2}(X)$, from definition 4.4 we have $S_{\alpha_R(\beta/X)} = R.S_\beta$, and from definition 4.2 we have $P_{\alpha_R(X)}(X) = R$,
- $R = R_1^*$: let $\alpha_R(X) = \nu Y.\alpha_{R_1}(X/Y) \wedge X$. Since by induction hypothesis $P_{S_{\alpha_{R_1}(Y/X)}} = R_1.S_\beta$, we have by definition 4.4 that $S_{\alpha_(\beta/X)} = R_1^*.S_\beta = R.S_\beta$. It follows immediately from definition 4.2 that $P_{\alpha_R(X)}(X) = R$.

□

Lemma 4.12. *For all modal specification S, it is possible to construct a sentence β_S of L_ν such that S and β_S have the same sets of models.*

Proof. From theorem 3.15, we have a decomposition of S from which we construct a formula β_S such that $S_{\beta_S} = S$, the only nontrivial operator being the language-prefixing one which is given by lemma 4.11. □

Example 4.13. *Let S be the modal specification of figure 2, the decomposition of S is:*

$$S = S_{\not\rightarrow^b} \cup a.(a.(b.a)^*.S_{\rightarrow^b} \cap b.(a.b)^*.S_{\rightarrow^a})$$

then the equivalent sentence is:

$$\beta_S = \not\rightarrow^b \wedge \rightarrow^a \wedge [a](\,[a]\nu X.(\,[b][a]X \wedge \rightarrow^b) \wedge [b]\nu Y.(\,[a][b]X \wedge \rightarrow^a)\,)$$

4.2.1 L_ν and modal specifications are equivalent

At this point, we can translate a sentence of L_ν into a modal specification and reciprocally, which is enough to prove the main theorem:

Proof. **(of theorem 4.1)**
If E is the set of models of a sentence β, then by corollary 4.7, $E \in mod(S_\beta)$. Reciprocally, if $E = mod(S)$ then by lemma 4.12, there exist β_S such that E is the set of models of β_S. □

A consequence of this proof is that, when considering modal specifications, the properties we can prove are immediately the same for L_ν; this is the case for the lattice structure of models stated in theorem 3.9.

4.3 conclusion

Modal specifications form a language based approach to the syntactic fragment L_ν of L_μ. They also provide an easy way to extract more structural fragments requiring some restricting properties for their components. In our future work, we introduce a hierarchical partition of the set of modal specifications based on their structural properties. We study the decidability of unlabeled Petri nets synthesis from modal specifications regarding this hierarchy, giving an upper bound and a lower bound for the decidability of the synthesis problem.

References

[AN01] A. Arnold and D. Niwinski. *Rudiments of mu-calculus.* North-Holland, 2001.

Unité de recherche INRIA Rennes
IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399