

Logique et Formalisation du Raisonnement

cours de DEA

partie II - Logiques Non Classiques

Stéphane Demri

Laboratoire LEIBNIZ, UMR 5522

46 Avenue Félix Viallet

38031 Grenoble

email: demri@imag.fr

<http://leibniz.imag.fr/ATINF/Stephane.Demri/>

Novembre 1998

Cette partie du cours "Logique et Formalisation du Raisonnement" du D.E.A. Informatique, Systèmes et Communications de l'ENSIMAG et de l'Université Joseph Fourier (1998/1999) présente différentes logiques qui modélisent des aspects particuliers du raisonnement. Par opposition à la logique classique (du premier ou du second ordre) qui prétend davantage à l'universalité (et cela a un coût, par exemple l'indécidabilité), les logiques non-classiques qui seront présentées ont été conçues pour un type d'applications bien défini. Dans la suite on supposera connue la sémantique de la logique classique du premier ordre et du calcul propositionnel.

Diverses références bibliographiques sont fournies le long du cours. Il n'est absolument pas nécessaire de les consulter car le cours a été conçu pour être auto-suffisant. Cependant, pour ceux qui désirent quelques approfondissements ou qui préfèrent comprendre le cours à partir d'autres sources, consulter les références peut s'avérer utile.

1 Introduction aux logiques modales

Données historiques Le philosophe grec Aristote est reconnu comme le précurseur de la logique modale. Une proposition *catégorique* s'analyse comme l'affirmation ou la négation de l'inhérence d'un prédicat dans un sujet. Par contre, les propositions *modales* sont caractérisées par la présence en elles de *modes*, c'est-à-dire de termes qui modifient ou déterminent l'inhérence du prédicat.

Ces modes sont par exemple associées aux notions de nécessité, possibilité, contingence, impossibilité. Voici quelques exemples:

1. addition d'adverbe: "Ricardo viendra certainement";
2. proposition complétive: "Il est certain que Thierry viendra".

Il existe différents types de modalités, certains seront étudiés dans la suite.

1. modalités *ontiques* (aussi appelées *aléthiques*): "il est nécessaire (possible, impossible, ...) que ...";
2. modalités *temporelles*: "il a toujours été que le soleil brille", "il existe un instant dans le futur où la proposition p est fausse";
3. modalités *épistémiques*: "Nicolas sait que ...", "Olivier croit que Gilles ne sait pas si ... est vrai";
4. modalités *déontiques*: "Il est obligatoire ...", "Il est permis ...".

Prendre en considération plus de deux valeurs de vérité (au lieu des seules **Vrai** et **Faux**) est aussi un moyen de modifier le rapport entre un sujet et un prédicat, ce qui est à la base de l'étude des logiques *multi-valuées* (non abordées ici).

Le retour moderne de la logique modale est dû à C.I. Lewis (au début de ce siècle, vers 1915) qui proposa une forme d'implication qui soit plus "naturelle" que l'implication dite *matérielle* du calcul des propositions. En effet,

1. $p \Rightarrow q$ est toujours vrai si p est insatisfaisable;

2. $p \Rightarrow q$ est toujours vrai si q est une tautologie.

$p \prec q$ est définie comme une implication *stricte*, puisque interprétée par "Il est nécessaire que p implique q " (aussi noté $\Box(p \Rightarrow q)$).

Il faut noter qu'avant les systèmes de Lewis, les raisonnements utilisant des modalités étaient étudiés en logique philosophique alors qu'ensuite l'étude des logiques modales a été intégrée à la logique symbolique.

Lewis a défini différents systèmes à la Hilbert contenant l'opérateur d'implication stricte et ce n'est qu'au début des années soixante que la sémantique des mondes possibles a été découverte, principalement par S. Kripke¹. Actuellement les logiques modales (et certaines de leur extension) sont étudiées par exemple en Intelligence Artificielle (représentation des connaissances) et en Informatique Fondamentale (vérification et synthèse de programmes).

Systèmes modaux standard Soit $\text{For}_0 = \{p_1, p_2, \dots\}$ un ensemble de propositions atomiques. Les formules (mono)modales sont définies inductivement de la façon suivante:

$$\phi ::= \overbrace{p_i \mid \neg\phi \mid \phi_1 \wedge \phi_2}^{\text{calcul propositionnel}} \mid \overbrace{\Box\phi \mid \Diamond\phi}^{\text{partie modale}}$$

On peut aussi se passer de \Diamond et définir \Diamond ainsi: $\Diamond\phi \stackrel{\text{def}}{=} \neg\Box\neg\phi$. On dit aussi que \Diamond et \Box sont des opérateurs *duaux* (à mettre en rapport avec les quantificateurs \exists et \forall en logique classique). \top , \perp , \vee , \Rightarrow , et \Leftrightarrow sont aussi des abréviations. On note $\text{sub}(\phi)$ l'ensemble des *sous-formules* de ϕ .

Notation. Soit \mathbf{X} une catégorie syntaxique et \mathbf{O} un objet syntaxique. On note $\mathbf{X}(\mathbf{O})$ l'ensemble des éléments de \mathbf{X} qui apparaissent dans \mathbf{O} . Par exemple, $\text{For}_0(\phi)$ est l'ensemble des propositions atomiques qui apparaissent dans la formule ϕ .

La taille d'une formule ϕ , notée $|\phi|$, est le nombre de symboles apparaissant dans ϕ . Afin d'obtenir un codage succinct, pour chaque variable

¹La paternité de cette sémantique est aussi attribuée à d'autres logiciens mais c'est S. Kripke qui l'a rendue populaire et accessible.

propositionnelle p_i , i est codé en binaire. On renommera aussi les variables propositionnelles si nécessaire. Par exemple, si on désire savoir si $p_{2^{100}} \vee \neg p_{2^{100}}$ est valide, on peut renommer cette formule en $p_1 \vee \neg p_1$ sans craindre de ne pas préserver la validité, satisfaisabilité, ... qui sont des propriétés auxquelles on s'intéressera.

Definition 1.1. Le système modal à la Hilbert K (en l'honneur de S. Kripke) est composé des schémas d'axiomes

1. les tautologies du calcul propositionnel;
2. $\Box p \Rightarrow (\Box(p \Rightarrow q) \Rightarrow \Box q)$;
3. $\Diamond \phi \Leftrightarrow \neg \Box \neg \phi$;

et des règles d'inférence:

1. *modus ponens*: $\frac{\phi \quad \phi \Rightarrow \psi}{\psi}$;
2. *nécessitation*: $\frac{\phi}{\Box \phi}$.

On note \vdash_K l'ensemble des théorèmes de K. ∇

Une *dérivation* du système K (une définition similaire est adoptée pour les autres systèmes présentés dans la suite) est une séquence $\langle \phi_1, \dots, \phi_n \rangle$ telle pour $i \in \{1, \dots, n\}$,

- soit ϕ_i est une instance d'un schéma d'axiomes de K;
- soit il existe $j < i$ tel que $\phi_i = \Box \phi_j$;
- soit il existe $j, j' < i$ tels qu'appliquer le *modus ponens* sur ϕ_j and $\phi_{j'}$ produit la formule ϕ_i .

Les théorèmes de K sont exactement les formules apparaissant dans une dérivation de K. Le schéma d'axiomes (2) peut être compris comme un *modus ponens* dans la portée d'opérateurs modaux. A la place des schémas d'axiomes (1) on peut se restreindre aux trois schémas d'axiomes suivants sans affaiblir le pouvoir déductif du système (avec en plus quelques schémas sur la définition de connecteurs et constantes logiques):

1. $p \Rightarrow (q \Rightarrow p)$;
2. $(p \Rightarrow (q \Rightarrow r)) \Rightarrow ((p \Rightarrow q) \Rightarrow (p \Rightarrow r))$;
3. $(\neg p \Rightarrow \neg q) \Rightarrow (q \Rightarrow p)$.

Dans l'hypothèse où l'opérateur \diamond n'est pas primitif dans le langage, le schéma d'axiomes (3) doit être supprimé dans la définition de K . Une dernière remarque sur \vdash_K : il n'est pas nécessaire d'avoir une règle de substitution uniforme car le système est défini à partir de schémas d'axiomes et non d'axiomes. On peut montrer par exemple que la règle $\frac{\phi \Rightarrow \psi}{\Box \phi \Rightarrow \Box \psi}$ est *admissible*, c'est-à-dire qu'ajouter cette règle au système K n'augmente pas le pouvoir déductif du système. Supposons que $\vdash_K \phi \Rightarrow \psi$. En appliquant la règle de nécessité, nous obtenons que $\vdash_K \Box(\phi \Rightarrow \psi)$. On peut facilement montrer que $(p \Rightarrow (q \Rightarrow q')) \Rightarrow (q \Rightarrow (p \Rightarrow q'))$ est une tautologie du calcul propositionnel. En utilisant le schéma d'axiomes (1) et en remplaçant p [resp. q, q'] par $\Box\phi$ [resp. $\Box(\phi \Rightarrow \psi), \Box\psi$], on déduit que

$$\vdash_K (\Box\phi \Rightarrow (\Box(\phi \Rightarrow \psi) \Rightarrow \Box\psi)) \Rightarrow (\Box(\phi \Rightarrow \psi) \Rightarrow (\Box\phi \Rightarrow \Box\psi))$$

Or, $\vdash_K \Box\phi \Rightarrow (\Box(\phi \Rightarrow \psi) \Rightarrow \Box\psi)$ en instanciant le schéma d'axiomes (2). On utilise alors la règle de *modus ponens* pour établir $\vdash_K \Box(\phi \Rightarrow \psi) \Rightarrow (\Box\phi \Rightarrow \Box\psi)$. En utilisant à nouveau la règle de *modus ponens* sur $\Box(\phi \Rightarrow \psi)$ (voir le début du raisonnement) et $\Box(\phi \Rightarrow \psi) \Rightarrow (\Box\phi \Rightarrow \Box\psi)$ on a donc $\vdash_K \Box\phi \Rightarrow \Box\psi$.

Parmi les autres systèmes modaux standard, on peut citer:

1. $T \stackrel{\text{def}}{=} K$ plus le schéma d'axiomes $\Box p \Rightarrow p$;
2. $D \stackrel{\text{def}}{=} K$ plus le schéma d'axiomes $\Box p \Rightarrow \diamond p$;
3. $K4 \stackrel{\text{def}}{=} K$ plus le schéma d'axiomes $\Box p \Rightarrow \Box\Box p$;
4. $S4 \stackrel{\text{def}}{=} T$ plus le schéma d'axiomes $\Box p \Rightarrow \Box\Box p$;
5. $S5 \stackrel{\text{def}}{=} S4$ plus le schéma d'axiomes $p \Rightarrow \Box\diamond p$;
6. $G \stackrel{\text{def}}{=} K4$ plus le schéma d'axiomes $\Box(\Box p \Rightarrow p) \Rightarrow \Box p$.

Les nouveaux schémas d'axiomes admettent diverses interprétations, en voici quelques exemples:

1. $\Box p \Rightarrow \Box \Box p$: introspection positive;
2. $\Box p \Rightarrow \Box \Box p$: si une proposition peut être montrée, alors on peut montrer que la proposition peut être montrée (système auto-référent, cf la partie I du cours);
3. $\neg \Box p \Rightarrow \Box \neg \Box p$: introspection négative;
4. $\Box p \Rightarrow p$: on ne peut savoir une proposition fausse;
5. $\Box p \Rightarrow \Diamond p$: on croit ce que l'on sait, ce qui est obligatoire est permis, ce qui sera toujours vrai sera vrai un jour, ...;

Il est clair que ces systèmes sans sémantique peuvent avoir un intérêt pour la théorie de la preuve mais l'interprétation de l'opérateur \Box reste à définir.

La sémantique des mondes possibles

Definition 1.2. Un *cadre modal* $\mathcal{F} = (W, R)$ est une paire où W est un ensemble non-vide et R est une relation binaire sur W . ∇

\mathcal{F} est donc un graphe orienté avec au plus une arête entre deux noeuds.

Definition 1.3. Un *modèle de Kripke* est un triplet $\mathcal{M} = (W, R, v)$ tel que

1. W est un ensemble non-vide (les "mondes");
2. R est une relation binaire sur W ("relation d'accessibilité")
3. $v : W \rightarrow 2^{\text{For}_0}$ est une fonction d'interprétation. On utilisera aussi $v : \text{For}_0 \rightarrow 2^W$.

La *base* du modèle $\mathcal{M} = (W, R, v)$ est le cadre (W, R) . ∇

Un modèle de Kripke est donc un graphe orienté dont chaque noeud est étiqueté par un ensemble de propositions atomiques, c'est-à-dire chaque noeud du graphe est une interprétation du calcul propositionnel.

En ce qui concerne la sémantique des logiques *polymodales*, la notion de modèle de Kripke est étendue par exemple en considérant une famille de relations binaires ce qui revient à étiqueter aussi les arcs. Il existe même

des logiques modales où les relations peuvent être de dimension supérieure à deux mais dans ce cas les opérateurs modaux ne sont plus nécessairement unaires.

La formule ϕ est satisfaite dans le monde w du modèle \mathcal{M} ssi $\mathcal{M}, w \models \phi$ où la relation de satisfaction \models est définie inductivement de la façon suivante:

1. $\mathcal{M}, w \models p_i \stackrel{\text{def}}{\Leftrightarrow} w \in v(p_i)$;
2. $\mathcal{M}, w \models \neg\phi \stackrel{\text{def}}{\Leftrightarrow} \mathcal{M}, w \not\models \phi$;
3. $\mathcal{M}, w \models \phi_1 \wedge \phi_2 \stackrel{\text{def}}{\Leftrightarrow} \mathcal{M}, w \models \phi_1$ et $\mathcal{M}, w \models \phi_2$;
4. $\mathcal{M}, w \models \Box\phi \stackrel{\text{def}}{\Leftrightarrow}$ pour tous les $w' \in R(w)$, $\mathcal{M}, w' \models \phi$;
5. $\mathcal{M}, w \models \Diamond\phi \stackrel{\text{def}}{\Leftrightarrow}$ il existe $w' \in R(w)$ tel que $\mathcal{M}, w' \models \phi$.

avec $R(w) \stackrel{\text{def}}{=} \{w' \in W : (w, w') \in R\}$. Par extension, $v(\phi) \stackrel{\text{def}}{=} \{w \in W : \mathcal{M}, w \models \phi\}$.

Voici quelques définitions supplémentaires relatives aux notions de validité et satisfaisabilité.

Soit Mod un ensemble de modèles de Kripke.

1. Une formule est *Mod-satisfaisable* $\stackrel{\text{def}}{\Leftrightarrow}$ il existe $\mathcal{M} \in Mod$ et $w \in \mathcal{M}$ tels que $\mathcal{M}, w \models \phi$.
2. Une formule ϕ est *valide dans le modèle* \mathcal{M} $\stackrel{\text{def}}{\Leftrightarrow} v(\phi) = W$.
3. Une formule ϕ est *Mod-valide* $\stackrel{\text{def}}{\Leftrightarrow}$ ϕ est valide dans tous les modèles de Mod .
4. Une formule ϕ est *valide dans le cadre modal* $\mathcal{F} = (W, R)$ $\stackrel{\text{def}}{\Leftrightarrow}$ ϕ est valide dans tous les modèles ayant pour base (W, R) .

Quelques références:

- B. Chellas. *Modal Logic: An Introduction*. Cambridge University Press, 1980.
- G. Hughes and M. Cresswell. *Introduction to Modal Logic*. Methuen, London, 1968.
- J. Hintikka. *Knowledge and Belief*. Cornell University Press, 1962.

Correspondance Le problème est le suivant. Soit ϕ une formule. Existe-t-il une propriété \mathcal{P} sur les relations binaires telle que pour tous les cadres (W, R) , ϕ est valide dans (W, R) ssi (W, R) satisfait \mathcal{P} ? On peut aussi considérer une propriété et se demander s'il existe une formule correspondante.

Proposition 1.1. Quelques résultats de correspondance classiques:

1. La formule $\Box p \Rightarrow p$ est valide dans (W, R) ssi R est réflexive sur W .
2. La formule $\Box p \Rightarrow \Diamond p$ est valide dans (W, R) ssi R est sérielle (pour chaque $w \in W$, $R(w) \neq \emptyset$).
3. La formule $\Box p \Rightarrow \Box \Box p$ est valide dans (W, R) ssi R est transitive.
4. La formule $p \Rightarrow \Box \Diamond p$ est valide dans (W, R) ssi R est symétrique.
5. La formule $\Box(\Box p \Rightarrow p) \Rightarrow \Box p$ est valide dans (W, R) ssi R est transitive et il n'y a pas de séquence infinie x_1, x_2, \dots d'éléments de W telle que pour $i \geq 1$, $(x_i, x_{i+1}) \in R$.

Preuve. A titre d'exemple, nous montrons (1).

(\rightarrow) Soit $\Box p \Rightarrow p$ valide dans (W, R) . Supposons par l'absurde que R ne soit pas réflexive. Il existe $w_0 \in W$ tel que $(w_0, w_0) \notin R$. Considérons le modèle $\mathcal{M}_0 = (W, R, v)$ tel que pour $w \in W$, $p \in v(w) \stackrel{\text{def}}{\Leftrightarrow} (w_0, w) \in R$. Comme $\Box p \Rightarrow p$ est valide dans (W, R) alors $\mathcal{M}_0, w_0 \models \Box p \Rightarrow p$. Par construction de v , $\mathcal{M}_0, w_0 \models \Box p$. Par conséquent $\mathcal{M}_0, w_0 \models p$, ce qui est en contradiction avec la définition de v .

(\leftarrow) Supposons que R soit réflexive dans le cadre (W, R) . Soit $\mathcal{M} = (W, R, v)$ un modèle et $w \in W$. Supposons que $\mathcal{M}, w \models \Box \phi$. Par définition de \models , pour $w' \in R(w)$, $\mathcal{M}, w' \models \phi$. En particulier $\mathcal{M}, w \models \phi$. C.Q.F.D.

Exercice 1.1. Montrer les points (2),(3),(4) et (5) de la proposition 1.1 en s'inspirant de la preuve de (1). Pour montrer (5), on pourra commencer par montrer que $\Box(\Box p \Rightarrow p) \Rightarrow \Box p$ est valide dans (W, R) ssi $\Diamond p \Rightarrow \Diamond(p \wedge \Box \neg p)$ est valide dans (W, R) .

Correction et complétude Un modèle \mathcal{M} est dit réflexif, ... ssi la relation binaire de \mathcal{M} est réflexive, ...

En utilisant, les résultats de correspondance et la construction du *modèle canonique*, on peut montrer les équivalences suivantes:

Proposition 1.2. Soit ϕ une formule modale.

1. $\vdash_K \phi$ ssi ϕ est valide pour tous les modèles de Kripke (noté Mod_K);
2. $\vdash_T \phi$ ssi ϕ est valide pour tous les modèles de Kripke réflexifs (noté Mod_T);
3. $\vdash_D \phi$ ssi ϕ est valide pour tous les modèles de Kripke sériels (noté Mod_D);
4. $\vdash_{K4} \phi$ ssi ϕ est valide pour tous les modèles de Kripke transitifs (noté Mod_{K4});
5. $\vdash_{S4} \phi$ ssi ϕ est valide pour tous les modèles de Kripke réflexifs et transitifs (noté Mod_{S4});
6. $\vdash_{S5} \phi$ ssi ϕ est valide pour tous les modèles de Kripke dont la relation d'accessibilité est une relation d'équivalence (noté Mod_{S5});
7. $\vdash_G \phi$ ssi ϕ est valide pour tous les modèles de Kripke dont la relation d'accessibilité est une relation transitive sans chemin infini (propriété *non exprimable* dans la logique classique du premier ordre).

Dans la suite une *logique modale* (normale) est un ensemble de formules fermé par modus ponens, substitution uniforme, nécessité et contenant les tautologies du calcul propositionnel ainsi que les instances de $(\Box p \Rightarrow \Box(p \Rightarrow q)) \Rightarrow \Box q$. Ainsi une logique modale peut être l'ensemble de théorèmes d'un système axiomatique ou encore l'ensemble des formules *Mod*-valides d'un certain ensemble de modèles de Kripke. La proposition 1.2 permet de concilier les approches syntaxique et sémantique.

Exercice 1.2. Montrer que les formules suivantes sont Mod_{S5} -valides:

- $\Box \Diamond \phi \Leftrightarrow \Diamond \phi$; $\Diamond \Diamond \phi \Leftrightarrow \Diamond \phi$;
- $\Box \Box \phi \Leftrightarrow \Box \phi$; $\Diamond \Box \phi \Leftrightarrow \Box \phi$.

Deduire que $\oplus_1 \dots \oplus_n \phi \Leftrightarrow \oplus_n \phi$ est Mod_{S5} -valide sachant que $n \geq 2$ et pour $i \in \{1, \dots, n\}$ \oplus_i vaut \Box ou \Diamond .

Décidabilité et complexité

Proposition 1.3. Pour $\mathcal{L} \in \{K, T, D, K4, S4, S5, G\}$, le problème de la \mathcal{L} -satisfaisabilité (en fait $Mod_{\mathcal{L}}$ -satisfaisabilité) est décidable.

On peut montrer ce résultat en utilisant la technique de filtration mais il existe aussi d'autres techniques. L'une d'entre elles consiste à utiliser des traductions dans des fragments décidables de la logique classique (cela ne marche pas pour G).

Proposition 1.4. Pour $\mathcal{L} \in \{K, T, D, K4, S4\}$, le problème de la \mathcal{L} -satisfaisabilité est **PSPACE**-complet: il peut être résolu par une machine de Turing déterministe en espace polynomial dans la taille de la formule initiale. De plus, tout problème de cette classe peut être réduit en temps polynomial à ce problème.

Ce résultat a été prouvé par R. Ladner (1979). Dans ce cours on s'intéresse à la complexité dans le pire des cas. Examinons le cas de la logique S5.

Proposition 1.5. Toute formule ϕ qui est S5-satisfaisable admet un modèle (W, R, v) tel que $R = W \times W$.

La preuve est laissée en exercice.

Proposition 1.6. Toute formule ϕ qui est S5-satisfaisable admet un modèle (W, R, v) tel que $card(W) \leq pm(\phi) + 1$.

$pm(\phi)$ est le nombre d'opérateurs modaux apparaissant dans ϕ ("poids modal").

Preuve. Sans perte de généralité on suppose que le seul opérateur modal dans ϕ est \Box . En effet, on peut toujours remplacer \Diamond par $\neg\Box\neg$ ce qui préserve la classe de modèles de la formule et ne modifie pas son poids modal.

Supposons que ϕ soit S5-satisfaisable. Il existe donc un modèle $\mathcal{M} = (W, R, v)$ et $w \in W$ tels que $\mathcal{M}, w \models \phi$ et $R = W \times W$ (cf Proposition 1.5). Soit X_ϕ l'ensemble des sous-formules de ϕ de la forme $\Box\psi$ tel que $\mathcal{M}, w \not\models \Box\psi$. Ainsi pour $\Box\psi \in X_\phi$, il existe $w_\psi \in W$ (un témoin) tel que $\mathcal{M}, w_\psi \not\models \psi$.

Soit $\mathcal{M}' = (W', R', v')$ le modèle tel que,

1. $W' \stackrel{\text{def}}{=} \{w\} \cup \{w_\psi : \Box\psi \in X_\phi\}$;
2. $R' \stackrel{\text{def}}{=} W' \times W'$;
3. v' est la restriction de v à W' , c'est-à-dire que pour $p \in \text{For}_0$, $v'(p) \stackrel{\text{def}}{=} v(p) \cap W'$.

Remarquez que $\text{card}(W') \leq pm(\phi) + 1$. On montre à présent que pour $w' \in W'$ et pour chaque sous-formule ψ de ϕ , $\mathcal{M}, w' \models \psi$ ssi $\mathcal{M}', w' \models \psi$ (par induction structurelle sur ψ).

Seul le cas $\psi = \Box\psi'$ est traité ici. Soit $w' \in W'$. Si $\mathcal{M}, w' \models \Box\psi'$ alors pour $w'' \in R(w') = W$, $\mathcal{M}, w'' \models \psi'$. En particulier, pour $w'' \in W' = R'(w') \subseteq R(w') = W$, $\mathcal{M}, w'' \models \psi'$. Par hypothèse d'induction, $\mathcal{M}', w'' \models \psi'$ pour $w'' \in R'(w')$, et donc $\mathcal{M}', w' \models \Box\psi'$.

Supposons à présent que $\mathcal{M}, w' \not\models \Box\psi'$. Comme R est une relation d'équivalence, on a alors $\mathcal{M}, w' \models \Box\neg\psi'$ et donc en particulier $\mathcal{M}, w \models \neg\Box\psi'$ ($(w', w) \in R$ car R est universelle). Par conséquent $\Box\psi' \in X_\phi$ et $\mathcal{M}, w_{\psi'} \not\models \psi'$. Par hypothèse d'induction, $\mathcal{M}', w_{\psi'} \not\models \psi'$. Comme $(w', w_{\psi'}) \in R'$, alors $\mathcal{M}', w' \not\models \Box\psi'$. C.Q.F.D.

Corollaire 1.7. Le problème de la S5-satisfaisabilité est dans la classe de complexité **NP**, c'est-à-dire il peut être résolu par une machine de Turing non-déterministe en temps polynomial.

En effet, il suffit de *deviner* une structure $\mathcal{M} = (W, R, v)$ telle que $R = W \times W$, $\text{card}(W)$ est inférieur à $pm(\phi) + 1$ (ces propriétés peuvent être vérifiées en temps polynomial) et de tester s'il existe $w \in W$ tel que $\mathcal{M}, w \models \phi$. Ce dernier point peut être vérifié en temps $O((pm(\phi) + 1)^2 \times |\phi|)$. Cette borne sera formellement établie dans la suite concernant le problème de vérification pour la logique temporelle CTL (le problème pour S5 n'est alors qu'un cas très particulier).

Proposition 1.8. Toute formule propositionnelle ϕ (sans opérateurs modaux) est satisfaisable dans le calcul propositionnel classique ssi ϕ est S5-satisfaisable

La preuve est laissée en exercice.

Corollaire 1.9. Le problème de la S5-satisfaisabilité est **NP**-difficile, c'est-à-dire chaque problème de la classe **NP** peut être réduit en temps polynomial au problème de la S5-satisfaisabilité.

Le problème de la S5-satisfaisabilité est donc **NP**-complet, par définition puisqu'il est dans **NP** et il est **NP**-difficile.

A titre indicatif, comme pour le calcul propositionnel, la S5-satisfaisabilité est dans la classe de complexité **P** (problème pouvant être résolu par une machine de Turing déterministe en temps polynomial) lorsque l'on se restreint à un ensemble fini de propositions atomiques (résultat dû à J. Halpern). Par contre, même avec une unique proposition atomique la K-satisfaisabilité et la S4-satisfaisabilité sont encore **PSPACE**-difficiles.

Exercice 1.3. Soit $X = \{p_{i_1}, \dots, p_{i_n}\}$ un ensemble fini de propositions atomiques. Les modèles $\mathcal{M}_1 = (W_1, R_1, v_1)$ et $\mathcal{M}_2 = (W_2, R_2, v_2)$ sont dits *X-isomorphes* $\stackrel{\text{def}}{\Leftrightarrow}$ il existe une bijection $f : W_1 \rightarrow W_2$ telle que:

- $R_2 = \{\langle f(x), f(y) \rangle : \langle x, y \rangle \in R_1\}$;
- pour chaque $p \in X$, $v_2(p) = \{f(x) : x \in v_1(p)\}$.

Montrer (par induction structurelle) que pour toute formule modale ϕ telle que $\text{sub}(\phi) \cap \text{For}_0 \subseteq X$, pour chaque $x \in W_1$, $\mathcal{M}_1, x \models \phi$ ssi $\mathcal{M}_2, f(x) \models \phi$.

Exercice 1.4. Soit Γ un ensemble fini de formules tel que si $\psi \in \Gamma$, alors $\text{sub}(\psi) \subseteq \Gamma$. Soit un modèle $\mathcal{M} = (W, R, v)$. On définit une relation $\equiv_\Gamma \subseteq W \times W$. Pour $x, y \in W$, $x \equiv_\Gamma y \stackrel{\text{def}}{\Leftrightarrow}$ pour $\phi \in \Gamma$, $\mathcal{M}, x \models \phi$ ssi $\mathcal{M}, y \models \phi$. \equiv_Γ est une relation d'équivalence et on note $|x|_\Gamma$ la classe d'équivalence de x . Le modèle $\mathcal{M}' = (W', R', v')$ est une Γ -filtration de $\mathcal{M} \stackrel{\text{def}}{\Leftrightarrow}$ les conditions suivantes sont vérifiées:

- $W' = \{|x|_\Gamma : x \in W\}$;
- si $\langle x, y \rangle \in R$, alors $\langle |x|_\Gamma, |y|_\Gamma \rangle \in R'$ (pour $x, y \in W$);
- si $\langle |x|_\Gamma, |y|_\Gamma \rangle \in R'$ et $\mathcal{M}, x \models \Box\psi$ pour $\Box\psi \in \Gamma$ alors $\mathcal{M}, y \models \psi$ (pour $x, y \in W$);
- pour $p \in \Gamma$, $v'(p) = \{|x|_\Gamma : x \in v(p)\}$.

On peut observer que $\text{card}(W') \leq 2^{\text{card}(\Gamma)}$.

1. Montrer (par induction structurelle) que si \mathcal{M}' est une Γ -filtration de \mathcal{M} alors pour $x \in W$ et pour $\phi \in \Gamma$, $\mathcal{M}, x \models \phi$ ssi $\mathcal{M}', x|_{\Gamma} \models \phi$.
2. Soit Γ un ensemble de sous-formules tel que pour $\psi \in \Gamma$, $\text{sub}(\psi) \subseteq \Gamma$. Soit $\mathcal{M} = (W, R, v)$ un modèle de Kripke. Le modèle \mathcal{M}' est défini ainsi:
 - $W' \stackrel{\text{def}}{=} \{x|_{\Gamma} : x \in W\}$;
 - pour $p \in \text{For}_0$, $v'(p) = \{x|_{\Gamma} : x \in v(p), p \in \Gamma\}$;
 - pour $x, y \in W$, $x|_{\Gamma} R' y|_{\Gamma} \stackrel{\text{def}}{\iff}$ il existe $x_0, y_0 \in W$ tels que $x_0|_{\Gamma} = x|_{\Gamma}$, $y_0|_{\Gamma} = y|_{\Gamma}$ et $x_0 R y_0$.

Montrer que \mathcal{M}' est une Γ -filtration de \mathcal{M} .

3. En déduire que si ϕ est K-satisfaisable alors il existe un modèle $\mathcal{M} = (W, R, v)$ et $w \in W$ tels que W est fini, $\text{card}(W) \leq 2^{|\phi|}$ et $\mathcal{M}, w \models \phi$.

Quelques références:

- J. van Benthem. Correspondence Theory. In D. Gabbay and F. Gunthner (eds.), Handbook of Philosophical Logic, Vol II, Reidel, Dordrecht, 1984, pp 167-247.
- G. Boolos. The logic of Provability. Cambridge University Press, 1993.
- R. Goldblatt. Logics of Time and Computation. CSLI Lecture Notes Number 7, CSLI Stanford, 1987.
- R. Ladner. The computational complexity of provability in systems of modal logic, SIAM Journal of Computing 6(3), 467-480, 1977.
- G. Hughes et M. Cresswell. A companion to Modal Logic. Methuen, London, 1968.
- D. Johnson. A catalog of complexity classes. In J. van Leeuwen, editor, Handbook of Theoretical Computer Science, vol. A, chapter 2, pages 67-161. Elsevier Science Publishers, 1990.

La traduction standard vers la logique classique De nombreuses logiques modales peuvent être traduites dans la logique classique pour ce qui est de la satisfaisabilité. C'est pourquoi on peut aussi voir certaines logiques modales comme des fragments de la logique classique.

Pour $k \geq 2$, on note $\text{FO}^k[=]$ le fragment de la logique classique avec k variables individuelles et l'égalité mais sans symbole fonctionnel. Dans la suite on se restreint même au vocabulaire suivant:

1. $\{\mathbf{P}_i : i \in \omega\}$ est un ensemble de symboles de prédicat unaire;
2. \mathbf{R} et $=$ (interprété comme l'identité) sont des symboles de prédicat binaire;
3. $\{\mathbf{x}_0, \dots, \mathbf{x}_{k-1}\}$ est un ensemble de variables individuelles de cardinalité k .

FO^k est défini comme $\text{FO}^k[=]$ mais sans égalité. Une structure pour $\text{FO}^k[=]$ (pour notre vocabulaire restreint), est une paire $\mathcal{M} = \langle D, m \rangle$ telle que D est un ensemble non-vide (le domaine) et m est une fonction d'interprétation telle que,

1. $m(\mathbf{P}_i) \subseteq D$ pour $i \in \omega$;
2. $m(\mathbf{R}) \subseteq D \times D$ et $m(=) = \{\langle a, a \rangle : a \in D\}$.

Une valuation $v_{\mathcal{M}}$ est une application $v_{\mathcal{M}} : \{\mathbf{x}_0, \dots, \mathbf{x}_{k-1}\} \rightarrow D$. On écrit $\mathcal{M} \models \phi [v_{\mathcal{M}}]$ pour dénoter que la formule ϕ est satisfaite dans \mathcal{M} avec la valuation $v_{\mathcal{M}}$. Par exemple, on rappelle que

$$\mathcal{M} \models \forall \mathbf{x}_i \phi[v_{\mathcal{M}}] \stackrel{\text{def}}{\Leftrightarrow} \text{pour tous les } w \in D, \mathcal{M} \models \phi[v_{\mathcal{M}}^{\mathbf{x}_i \leftarrow w}] \text{ où pour } j \neq i, v_{\mathcal{M}}(\mathbf{x}_j) = v_{\mathcal{M}}^{\mathbf{x}_i \leftarrow w}(\mathbf{x}_j) \text{ et } v_{\mathcal{M}}^{\mathbf{x}_i \leftarrow w}(\mathbf{x}_i) = w.$$

De même,

$$\mathcal{M} \models \exists \mathbf{x}_i \phi[v_{\mathcal{M}}] \stackrel{\text{def}}{\Leftrightarrow} \text{il existe } w \in D \text{ tel que } \mathcal{M} \models \phi[v_{\mathcal{M}}^{\mathbf{x}_i \leftarrow w}] \text{ où pour } j \neq i, v_{\mathcal{M}}(\mathbf{x}_j) = v_{\mathcal{M}}^{\mathbf{x}_i \leftarrow w}(\mathbf{x}_j) \text{ et } v_{\mathcal{M}}^{\mathbf{x}_i \leftarrow w}(\mathbf{x}_i) = w.$$

Ou encore, $\mathcal{M} \models \mathbf{P}_j(\mathbf{x}_i)[v_{\mathcal{M}}] \stackrel{\text{def}}{\Leftrightarrow} v_{\mathcal{M}}(\mathbf{x}_i) \in m(\mathbf{P}_j)$. On omet $[v_{\mathcal{M}}]$ lorsque ϕ est fermée, c'est-à-dire toute variable \mathbf{x}_i apparaissant dans une formule atomique est dans la portée d'une quantification de la forme $\forall \mathbf{x}_i$ ou $\exists \mathbf{x}_i$.

Il a été montré que $\text{FO}^2[=]$ est décidable (par M. Mortimer en 1975) et la satisfaisabilité est même **NEXPTIME**-complète. La borne supérieure de complexité est un résultat récent de E. Grädel, Ph. Kolaitis, et M. Vardi (1997) tandis que la borne inférieure de complexité a été montrée par H. Lewis en 1980.

L'idée de la traduction (étudiée par J. van Benthem dès le début des années 1980) consiste à exprimer dans FO^2 la quantification liée à l'interprétation de ' \Box ' en introduisant dans FO^2 le symbole de prédicat R .

Une logique modale \mathcal{L} (ensemble particulier de formules modales) est caractérisée par une classe de modèles $Mod \stackrel{\text{def}}{\Leftrightarrow} \mathcal{L} = \{\phi : \text{pour tous les } \mathcal{M} \in Mod, \mathcal{M} \models \phi\}$ (ssi pour $\phi \in \text{For}$, $\phi \in \mathcal{L}$ ssi ϕ est Mod -valide). Soit \mathcal{L} une logique modale caractérisée par une classe $Mod_{\mathcal{L}}$ de modèles de Kripke telle qu'il existe une formule fermée $\phi_{\mathcal{L}}$ de $\text{FO}^k[=]$ (construite sur les seuls symboles de prédicat R et $=$) pour $k \geq 2$ satisfaisant:

pour tous les cadres modaux (W, R) , $(W, R) \models \phi_{\mathcal{L}}$ (au sens de la logique classique) ssi tous les modèles ayant pour base (W, R) sont dans $Mod_{\mathcal{L}}$.

Les logiques $K, T, D, S4, S5$ appartiennent à cette classe de logiques modales et ce ne sont évidemment pas les seules. Par exemple, $\phi_T \stackrel{\text{def}}{=} \forall x_0 R(x_0, x_0)$ et $\phi_D \stackrel{\text{def}}{=} \forall x_0 \exists x_1 R(x_0, x_1)$. Par contre, G n'appartient pas à cette classe.

Soit t une application transformant une formule modale en une formule de FO^2 ($i \in \{0, 1\}$):

1. $t(p_j, \mathbf{x}_i) \stackrel{\text{def}}{=} P_j(\mathbf{x}_i)$;
2. t est homomorphique pour les connecteurs propositionnels, par exemple $t(\neg\phi, \mathbf{x}_i) \stackrel{\text{def}}{=} \neg t(\phi, \mathbf{x}_i)$;
3. $t(\Box\phi, \mathbf{x}_i) \stackrel{\text{def}}{=} \forall \mathbf{x}_{1-i} (R(\mathbf{x}_i, \mathbf{x}_{1-i}) \Rightarrow t(\phi, \mathbf{x}_{1-i}))$;
4. $t(\Diamond\phi, \mathbf{x}_i) \stackrel{\text{def}}{=} \exists \mathbf{x}_{1-i} R(\mathbf{x}_i, \mathbf{x}_{1-i}) \wedge t(\phi, \mathbf{x}_{1-i})$.

La traduction t utilise exactement deux variables individuelles, \mathbf{x}_0 et \mathbf{x}_1 (recyclage dynamique des variables). On définit alors T ainsi:

$$T(\phi) \stackrel{\text{def}}{=} \phi_{\mathcal{L}} \wedge \exists \mathbf{x}_0 t(\phi, \mathbf{x}_0)$$

Par exemple,

$$t(\diamond \diamond p_1, \mathbf{x}_0) \stackrel{\text{def}}{=} \exists \mathbf{x}_1 (R(\mathbf{x}_0, \mathbf{x}_1) \wedge (\exists \mathbf{x}_0 R(\mathbf{x}_1, \mathbf{x}_0) \wedge P_1(\mathbf{x}_0)))$$

Pour le cas particulier de la logique K, $T(\phi) \stackrel{\text{def}}{=} \exists \mathbf{x}_0 t(\phi, \mathbf{x}_0)$ car Mod_K est l'ensemble de tous les modèles de Kripke.

Proposition 1.10. ϕ est \mathcal{L} -satisfaisable ssi $T(\phi)$ est $FO^k[=]$ -satisfaisable.

Preuve. Supposons d'abord que ϕ soit \mathcal{L} -satisfaisable. Il existe donc un modèle $\mathcal{M} = (W, R, v) \in Mod_{\mathcal{L}}$ et $w_0 \in W$ tels que $\mathcal{M}, w_0 \models \phi$. Soit $\mathcal{M}' = \langle D, m \rangle$ la structure du 1^{er} ordre:

1. $D \stackrel{\text{def}}{=} W$;
2. pour $i \in \omega$, $m(P_i) \stackrel{\text{def}}{=} v(p_i)$;
3. $m(R) \stackrel{\text{def}}{=} R$.

Par définition de $Mod_{\mathcal{L}}$, $\mathcal{M}' \models \phi_{\mathcal{L}}$. Montrons que $\mathcal{M}' \models \exists \mathbf{x}_0 t(\phi, \mathbf{x}_0)$ ce qui impliquera $\mathcal{M}' \models T(\phi)$. En fait on montre (par induction structurale) que pour toute sous-formule ψ de ϕ , pour $w \in W$ et pour $i \in \{0, 1\}$, $\mathcal{M}, w \models \psi$ ssi $\mathcal{M}' \models t(\psi, \mathbf{x}_i)$ [$\mathbf{x}_i \leftarrow w$]. $\mathbf{x}_i \leftarrow w$ dénote une valuation $v_{\mathcal{M}'} : \{\mathbf{x}_0, \dots, \mathbf{x}_{k-1}\} \rightarrow D$ telle que $v_{\mathcal{M}'}(\mathbf{x}_i) = w$. On aura bien $\mathcal{M}' \models \exists \mathbf{x}_0 t(\phi, \mathbf{x}_0)$ puisque $\mathcal{M}, w_0 \models \phi$.

Cas de base: $\psi = p_j$

$\mathcal{M}, w \models p_j$ ssi $w \in v(p_j)$ ssi $w \in m(P_j)$ ssi $\mathcal{M}' \models P_j(\mathbf{x}_i)$ [$\mathbf{x}_i \leftarrow w$].

Etape d'induction

Le cas où ψ est dominée par un connecteur propositionnel est omis car la preuve ne pose pas de difficulté. Seul le cas $\psi = \Box \psi_1$ est traité ici.

$\mathcal{M}, w \models \Box \psi_1$ ssi pour tous les $w' \in R(w)$, $\mathcal{M}, w' \models \psi_1$ ssi pour tous les $w' \in m(R)(w)$, $\mathcal{M}, w' \models \psi_1$ ssi pour tous les $w' \in m(R)(w)$, $\mathcal{M}' \models t(\psi_1, \mathbf{x}_{1-i})$ [$\mathbf{x}_{1-i} \leftarrow w'$] (par hypothèse d'induction) ssi

$$\mathcal{M}' \models \forall \mathbf{x}_{1-i} (R(\mathbf{x}_i, \mathbf{x}_{1-i}) \Rightarrow t(\psi_1, \mathbf{x}_{1-i}))$$
 [$\mathbf{x}_i \leftarrow w$]

ssi

$$\mathcal{M}' \models t(\Box\psi_1, \mathbf{x}_i) [\mathbf{x}_i \leftarrow w]$$

Supposons à présent que $\mathcal{M}' \models T(\phi)$ pour \mathcal{M}' une structure du 1^{er} ordre (on garde les notations précédentes). On note w_0 un élément du domaine D tel que $\mathcal{M}' \models t(\phi, \mathbf{x}_0) [\mathbf{x}_0 \leftarrow w_0]$. Soit $\mathcal{M} = (W, R, v)$ le modèle tel que:

1. $W \stackrel{\text{def}}{=} D$;
2. pour $i \in \omega$, $v(p_i) \stackrel{\text{def}}{=} m(\mathbf{P}_i)$;
3. $R \stackrel{\text{def}}{=} m(\mathbf{R})$.

Comme $\mathcal{M}' \models \phi_{\mathcal{L}}$ alors $\mathcal{M} \in \text{Mod}_{\mathcal{L}}$. On peut montrer par induction structurale (comme pour le cas précédent) que $\mathcal{M}, w_0 \models \phi$. Par conséquent, ϕ est \mathcal{L} -satisfaisable. C.Q.F.D.

On peut modifier T pour d'autres types de logiques modales, en particulier pour des logiques multimodales (avec plusieurs opérateurs modaux dépendants ou indépendants). Pour la mécanisation des logiques modales cette traduction a le double avantage,

1. de nécessiter l'existence d'un *unique* démonstrateur;
2. et d'être suffisamment naturelle et flexible.

Parmi les inconvénients on peut noter:

1. La logique classique est indécidable. Cependant pour les logiques K, T, D on traduit dans un fragment qui est connu pour être décidable, en l'occurrence FO^2 . Il faut rappeler aussi que le problème de la K-satisfaisabilité est dans **PSPACE** alors que FO^2 a un problème de satisfaisabilité **EXPTIME**-difficile (**PSPACE** \subseteq **EXPTIME**) .
2. Toutes les propriétés de la relation d'accessibilité ne sont pas exprimables dans la logique classique (R bien fondée par exemple). La validité de G ne peut être traduite dans la logique classique avec la traduction relationnelle.
3. On peut aussi souhaiter pour des raisons d'efficacité que le raisonnement sur les propriétés de R (codées dans $\phi_{\mathcal{L}}$) soit disjoint du reste du calcul.

Exercice 1.5. On étend le langage mono-modal étudié dans cette section, en considérant aussi un ensemble dénombrable $\text{For}_0^N = \{p_1^N, p_2^N, \dots\}$ de *noms*. Chaque nom se comporte comme une variable propositionnelle si ce n'est que chaque nom p_i^N est vérifié dans un *unique* état du modèle. Cela signifie qu'un modèle est de la forme (W, R, v) tel que $v(p_i^N)$ est un singleton pour chaque nom p_i^N . Soit K^N l'extension de la logique modale K (voir les sections précédentes) à laquelle on a ajouté des noms.

1. Étendre la traduction T pour K^N .
2. Sachant que $\text{FO}^2[=]$ a un problème de satisfaisabilité décidable, en déduire que le problème de satisfaisabilité pour K^N est décidable.

Quelques références:

- C. Morgan. Methods for automated theorem proving in non classical logics. IEEE Transactions on Computers, 25(8):852-862, 1976.
- J. van Benthem. Modal logic and classical logic. Bibliopolis, 1983.
- G. Gargov et V. Goranko. Modal logic with names. Journal of Philosophical Logic, 22(6):607-636, December 1993.
- E. Grädel, Ph. Kolaitis, M. Vardi. On the decision problem for two-variable first-order logic. Bulletin of Symbolic Logic, 3(1):53-69, 1997.

2 Logiques temporelles

2.1 La logique CTL

CTL ("Computation Tree Logic") est une logique pour la spécification et la vérification formelles de systèmes réactifs. Elle a été introduite par A. Emerson et J. Halpern en 1985. Un langage de spécification formelle permet

1. de définir mathématiquement la correction de programmes;
2. de s'exprimer rigoureusement et clairement;
3. ou encore de faire des preuves que par exemple une spécification vérifie une certaine propriété.

Exemple de systèmes réactifs: protocole de communication, système d'exploitation. En fait les systèmes réactifs,

1. ne terminent pas forcément;
2. ne calculent pas un résultat mais plutôt maintiennent une interaction;
3. et gèrent des communications extérieures en cours de route.

La sémantique de CTL utilise la sémantique des mondes possibles. Une structure est composée d'un ensemble d'états (modélisant les états du système) et d'une relation binaire qui correspond à la relation de transition entre les états du système/programme. Par ailleurs CTL (et ses variantes) ne mentionne pas explicitement les programmes mais opère directement sur les instructions d'un programme donné. Cela est particulièrement bien adapté pour raisonner avec un unique programme (à la différence des *logiques dynamiques* qui ne seront pas étudiées ici). D'un point de vue historique, il semblerait que ce soit A. Pnueli qui ait eu l'idée d'utiliser le cadre des logiques temporelles pour étudier le comportement de programmes (et davantage). Un de ses papiers de 1977 témoigne de son approche novatrice.

Syntaxe Soit $\text{For}_0 = \{p_1, p_2, \dots\}$ un ensemble de propositions atomiques. Les formules de CTL sont définies inductivement de la façon suivante:

$$\phi ::= p_i \mid \neg\phi \mid \phi_1 \wedge \phi_2 \mid \exists X\phi \mid \exists G\phi \mid \exists(\phi_1 U \phi_2)$$

Sémantique Les CTL-modèles sont les structures de Kripke propositionnelles dans l'acceptation standard du terme.

Definition 2.1. Un *CTL-modèle* est une structure $\mathcal{M} = (W, R, v)$ où

1. W est un ensemble non-vide d'états;
2. R est une relation binaire sur W . On suppose de plus que R est sérielle; pour chaque $w \in W$, il existe $w' \in W$ tel que $(w, w') \in R$;
3. $v : p \rightarrow 2^W$ est une fonction d'interprétation.

Un chemin de \mathcal{M} est une séquence $w_0, w_1, \dots, w_n, \dots$ (finie ou infinie) telle que pour $i \geq 0$, $(w_i, w_{i+1}) \in R$. ∇

La formule ϕ est satisfaite dans l'état w du modèle $\mathcal{M} \stackrel{\text{def}}{\models} \mathcal{M}, w \models \phi$ où la relation de satisfaction \models est définie inductivement de la façon suivante:

1. $\mathcal{M}, w \models p_i \stackrel{\text{def}}{\iff} w \in v(p_i)$;
2. $\mathcal{M}, w \models \neg\phi \stackrel{\text{def}}{\iff} \mathcal{M}, w \not\models \phi$;
3. $\mathcal{M}, w \models \phi_1 \wedge \phi_2 \stackrel{\text{def}}{\iff} \mathcal{M}, w \models \phi_1$ et $\mathcal{M}, w \models \phi_2$;
4. $\mathcal{M}, w \models \exists X\phi \stackrel{\text{def}}{\iff}$ il existe $w' \in R(w)$ tel que $\mathcal{M}, w' \models \phi$ ($\exists X$ a la sémantique de \diamond);
5. $\mathcal{M}, w \models \exists G\phi_1 \stackrel{\text{def}}{\iff}$ il existe un chemin infini w_0, w_1, \dots tel que $w_0 = w$ et pour $k \geq 0$, $\mathcal{M}, w_k \models \phi_1$;
6. $\mathcal{M}, w \models \exists(\phi_1 U \phi_2) \stackrel{\text{def}}{\iff}$ il existe un chemin infini $w = w_0, w_1, \dots$ et s'il existe $k \geq 0$ tel que $\mathcal{M}, w_k \models \phi_2$ et pour $0 \leq i < k$, $\mathcal{M}, w_i \models \phi_1$.

Les abréviations suivantes sont aussi courantes:

1. $\top \stackrel{\text{def}}{=} p_1 \vee \neg p_1$;
2. $\forall X\phi_1 \stackrel{\text{def}}{=} \neg\exists X\neg\phi_1$; $\forall F\phi \stackrel{\text{def}}{=} \neg\exists G\neg\phi$;
3. $\exists F\phi \stackrel{\text{def}}{=} \exists(\top U \phi)$; $\forall G\phi \stackrel{\text{def}}{=} \neg\exists F\neg\phi$;
4. $\forall(\phi_1 U \phi_2) \stackrel{\text{def}}{=} \neg(\exists(\neg\phi_2 U (\neg\phi_1 \wedge \neg\phi_2)) \vee \exists G\neg\phi_2)$.

Comme les abréviations ci-dessus le suggèrent, on peut définir le langage de CTL à partir de divers opérateurs temporels. Notre choix ici est guidé par la simplification de quelques développements techniques dans la suite. Chaque opérateur temporel quantifie sur les chemins et "ensuite" énonce une propriété sur les chemins.

Exercice 2.1. Vérifier que $\mathcal{M}, w \models \forall(\phi_1 U \phi_2)$ ssi pour tous les chemins infinis $w = w_0, w_1, \dots$, il existe $k \geq 0$ tel que $\mathcal{M}, w_k \models \phi_2$ et pour $0 \leq i < k$, $\mathcal{M}, w_i \models \phi_1$.

Expression de quelques propriétés

1. Une condition ϕ ne peut jamais être vérifiée: $\neg\exists F\phi$ (ϕ peut être que deux processus sont dans une région critique en même temps, dans le cas de partage de ressource);
2. A tout moment, il existe un instant ultérieur où une condition ϕ est vérifiée: $\forall G\exists F\phi$ (ϕ peut être qu'un des deux processus est dans une région critique);
3. Pour toutes les exécutions possibles, on vérifie un jour la condition ϕ : $\forall F\phi$.

Problèmes Les problèmes auxquels on s'intéresse généralement pour CTL sont les suivants:

1. Satisfaisabilité: pour une formule ϕ donnée, est-ce qu'il existe un CTL-modèle $\mathcal{M} = (W, R, v)$ et $w \in W$ tel que $\mathcal{M}, w \models \phi$?
(est-ce qu'une spécification ϕ admet un modèle?)
2. Validité: pour une formule ϕ donnée, est-ce que pour tous les CTL-modèles $\mathcal{M} = (W, R, v)$ et tous les $w \in W$, $\mathcal{M}, w \models \phi$?
(soient ϕ une spécification et ψ une propriété, est-ce que $\phi \Rightarrow \psi$ est valide?)
3. Vérification: pour un CTL-modèle fini $\mathcal{M} = (W, R, v)$ et une formule ϕ donnée, déterminer l'ensemble $\{w : \mathcal{M}, w \models \phi\}$. Une variante consiste à fixer $w \in W$ et à savoir si $\mathcal{M}, w \models \phi$.
(est-ce que l'état initial w d'un programme \mathcal{M} , vérifie la spécification ϕ ?)

Complexité algorithmique

Proposition 2.1. Le problème de la CTL-satisfaisabilité est **EXPTIME**-complet: il peut être résolu par une machine de Turing déterministe en temps exponentiel dans la taille de la formule initiale. De plus, tout problème de cette classe peut être réduit en temps polynomial au problème de la CTL-satisfaisabilité.

On peut aussi montrer qu'une formule est CTL-satisfaisable ssi elle est satisfaisable dans un CTL-modèle fini.

Proposition 2.2. Soient $\mathcal{M} = (W, R, v)$ un CTL-modèle fini et ϕ une formule. Déterminer l'ensemble $\{w : \mathcal{M}, w \models \phi\}$ peut être calculé en temps $O((\text{card}(R) + \text{card}(W)) \times |\phi|)$.

Par conséquent le problème de la vérification pour CTL est dans **P** (en fait c'est bilinéaire en la taille de la formule et du modèle). La propriété énoncée dans la proposition 2.2 est certainement une raison majeure pour comprendre l'utilisation intensive qui a été faite de CTL pour la vérification de programmes ayant un nombre fini d'états.

Preuve. Soient $\mathcal{M} = (W, R, v)$ un CTL-modèle fini et ϕ une CTL-formule. Le graphe orienté (W, R) est supposé donné par les listes des voisins (de taille $O(\text{card}(R) + \text{card}(W))$) tandis que l'interprétation v est représentée par un vecteur de longueur $\text{card}(W)$ dont la i^{ieme} case contient les variables propositionnelles (de ϕ) vérifiées dans l'état i (on a ordonné de façon arbitraire les états de W). La représentation de v est de taille $O(\text{card}(W) \times |\phi|)$.

Soient ϕ_1, \dots, ϕ_k les sous-formules de ϕ énumérées par taille croissante. En cas de conflit, on choisit un ordre arbitraire. Par conséquent,

1. $\phi_k = \phi$;
2. ϕ_1 est une proposition atomique;
3. si ϕ_i est une sous-formule stricte de ϕ_j alors $i < j$;
4. $k \leq |\phi|$.

Pour chaque $w \in W$, on construit un ensemble de formules $l(w)$ tel que

1. pour $i \in \{1, \dots, k\}$ soit $\phi_i \in l(w)$, soit $\neg\phi_i \in l(w)$, mais pas les deux à la fois;
2. pour $\psi \in \{\phi_1, \dots, \phi_k, \neg\phi_1, \dots, \neg\phi_k\}$, $\psi \in l(w)$ ssi $\mathcal{M}, w \models \psi$.

Pour chaque $i \in \{1, \dots, k\}$, et pour chaque $w \in W$ on met soit ϕ_i dans $l(w)$, soit $\neg\phi_i$ dans $l(w)$. Les ensembles de formules $l(w)$ ont pour valeur initiale l'ensemble vide. Six cas sont distingués et chaque étape (pour un

$i \in \{1, \dots, k\}$) se calcule en temps $O(\text{card}(W) + \text{card}(R))$.

Cas 1: ϕ_i est une formule atomique

Pour $w \in W$, si $w \in v(\phi_i)$ alors mettre ϕ_i dans $l(w)$ sinon mettre $\neg\phi_i$ dans $l(w)$.

Cas 2: $\phi_i = \neg\phi_{i_1}$ pour $i_1 < i$

Pour $w \in W$, mettre $\neg\phi_i$ dans $l(w)$ si $\phi_{i_1} \in l(w)$ sinon ne rien faire (ϕ_i est alors déjà dans $l(w)$).

Cas 3: $\phi_i = \phi_{i_1} \wedge \phi_{i_2}$ pour $i_1 < i, i_2 < i$

Pour $w \in W$, mettre ϕ_i dans $l(w)$ si $\{\phi_{i_1}, \phi_{i_2}\} \subseteq l(w)$ sinon mettre $\neg\phi_i$ dans $l(w)$.

Cas 4: $\phi_i = \exists X \phi_{i_1}$ pour $i_1 < i$

Pour $w \in W$, s'il existe $w' \in R(w)$ tel que ϕ_{i_1} est dans $l(w')$ alors mettre ϕ_i dans $l(w)$, sinon mettre $\neg\phi_i$ dans $l(w)$.

Cas 5: $\phi_i = \exists(\phi_{i_1} U \phi_{i_2})$ pour $i_1 < i, i_2 < i$

Pour $j \in \{1, 2\}$ on définit,

$$W_j \stackrel{\text{def}}{=} \{w \in W : \phi_{i_j} \in l(w)\}$$

Soit $\mathcal{M}' \stackrel{\text{def}}{=} (W', R', v')$ le modèle de Kripke tel que

1. $W' \stackrel{\text{def}}{=} W_1 \cup W_2$;
2. $R' \stackrel{\text{def}}{=} R^{-1} \cap W' \times W'$;
3. v' est la restriction de v à W' .

Pour $w \in W$, s'il existe $w' \in W_2$ tel que $w \in (R')^*(w')$ alors mettre ϕ_i dans $l(w)$ sinon mettre $\neg\phi_i$ dans $l(w)$. Pour montrer que cette étape se calcule en temps $O(\text{card}(W) + \text{card}(R))$ il faut utiliser le résultat suivant de la théorie des graphes:

Lemme 2.3. Soit $G = (W, R)$ un graphe orienté représenté par les listes de voisins et $\emptyset \neq X \subseteq W$. Déterminer l'ensemble $\bigcup\{R^+(r) : r \in X\}$ se calcule en temps $O(\text{card}(W) + \text{card}(R))$ où R^+ est la fermeture transitive de R (plus petite relation transitive contenant R).

Cas 6: $\phi_i = \exists G\phi_{i_1}$ pour $i_1 < i$

On définit de façon similaire au cas précédent,

$$W' \stackrel{\text{def}}{=} \{w \in W : \phi_{i_1} \in l(w)\}$$

Soit $\mathcal{M}' = (W', R', v')$ la restriction de \mathcal{M} à W' , c'est-à-dire pour $p \in \text{For}_0$, $v'(p) \stackrel{\text{def}}{=} v(p) \cap W'$ et $R' \stackrel{\text{def}}{=} R \cap (W' \times W')$.

On montre que pour $w \in W$, $\mathcal{M}, w \models \phi_i$ ssi

(I) $w \in W'$ et

(II) il existe un chemin (fini) dans \mathcal{M}' de w vers un état w' qui appartienne à une composante fortement connexe non triviale du graphe (W', R') .

Une *composante fortement connexe non triviale* C de (W', R') est un sous-ensemble de W' tel que,

1. pour $w' \neq w'' \in C$, il existe un R' -chemin de w' à w'' et un R' -chemin de w'' à w' (C fortement connexe);
2. $\text{card}(C) > 1$ ou bien $C = \{w'\}$ et $(w', w') \in R'$ (C non-triviale).

Supposons que $\mathcal{M}, w \models \exists G\phi_{i_1}$. Evidemment $w \in W'$. Soit w_0, w_1, \dots un chemin infini de \mathcal{M} tel que $w_0 = w$ et pour $j \geq 0$, $\mathcal{M}, w_j \models \phi_{i_1}$. Il existe $n \geq 0$ tel que pour $j \geq n$, w_j apparait un nombre infini de fois sur le chemin w_n, w_{n+1}, \dots . Les éléments de w_0, \dots, w_{n-1} (si $n = 0$ il s'agit de la séquence vide) sont contenus dans W' .

Soit C l'ensemble de états apparaissant dans w_n, w_{n+1}, \dots . On peut montrer que C est une composante fortement connexe non triviale. Si C est un singleton alors c'est immédiat. Sinon, en prenant $x, y \in C$, on peut toujours trouver un R' -chemin de x à y et de y à x car ils apparaissent un nombre infini de fois.

Supposons à présent que (I) et (II) soient vérifiées. Soit ch_1 le R' -chemin fini de w à w' . Soit ch_2 un R' -chemin fini de longueur au moins 1 entre w' et w' (d'après les propriétés de C). Tous les états sur le chemin $ch_1ch_2^\omega$ satisfont ϕ_{i_1} . Comme $ch_1ch_2^\omega$ (c'est-à-dire $ch_1ch_2ch_2ch_2 \dots$) est aussi un R -chemin

commençant en w , alors $\mathcal{M}, w \models \phi_i$.

On peut à présent conclure la preuve. Soit C_1, \dots, C_n une partition de W' tel que chaque C_i est un composante fortement connexe maximale au sens de l'inclusion ensembliste. Pour montrer que cette étape se calcule en temps $O(\text{card}(W) + \text{card}(R))$ il faut utiliser le résultat suivant issu de la théorie des graphes:

Lemme 2.4. Soit $G = (W, R)$ un graphe orienté représenté par les listes de voisins. Déterminer la partition des composantes fortement connexes maximales se calcule en temps $O(\text{card}(W) + \text{card}(R))$.

On peut consulter les livres de Aho, A., Hopcroft, J. et Ullman, J. intitulés "Data structures and algorithms" (1983, Amsterdam : Addison-Wesley) et "Design and analysis of computer algorithms" (1974, Amsterdam : Addison-Wesley) pour savoir comment de les lemmes concernant la théorie des graphes peuvent être démontrés.

On note W'' l'union des C_i telle que C_i est non-triviale. Pour chaque $w \in W$, si $w \in W'$ et s'il existe $w' \in W''$ tel que $w \in (R'^{-1})^*(w')$ alors mettre ϕ_i dans $l(w)$ sinon mettre $\neg\phi_i$ dans $l(w)$. Comme pour le cas précédent, on peut montrer que cette étape se calcule aussi en temps $O(\text{card}(W) + \text{card}(R))$. C.Q.F.D.

Quelques références:

- A. Pnueli. The temporal logic of programs. In 18th Annual Symposium on Foundations of Computer Science, pp 46-57, 1977.
- E. Emerson et J. Halpern. Decision procedures and expressiveness in the temporal logic of branching time. Journal of Computer and Systems Sciences, 30 pp 1-24, 1985.
- Z. Manna et A. Pnueli. The temporal logic of reactive and concurrent systems: Specification. Springer-Verlag, 1992.
- R. Goldblatt. Logics of Time and Computation. CSLI Lecture Notes Number 7, CSLI Stanford, 1987.
- A. Emerson. Temporal and modal logic. In Handbook of Theoretical Computer Science (ed.) van Leeuwen, J. pp 996-1072. Elsevier Science Publishers B.V., 1990.

Correction: (Exercice 1.1) A titre d'exemple (4) est démontré.

(\rightarrow) Soit $p \Rightarrow \Box \Diamond p$ valide dans (W, R) . Supposons que R ne soit pas symétrique. Il existe $w_0, w_1 \in W$ tel que $(w_0, w_1) \in R$ et $(w_1, w_0) \notin R$. Considérons le modèle $\mathcal{M}_0 = (W, R, v)$ tel que pour $w \in W$, $p \in v(w) \stackrel{\text{def}}{\Leftrightarrow} (w_1, w) \notin R$. Comme $p \Rightarrow \Box \Diamond p$ est valide dans (W, R) alors $\mathcal{M}_0, w_0 \models p \Rightarrow \Box \Diamond p$. Par construction de v , $\mathcal{M}_0, w_1 \models \Box \neg p$ et donc $\mathcal{M}_0, w_0 \models \Diamond \Box \neg p$, c'est-à-dire $\mathcal{M}_0, w_0 \models \neg \Box \Diamond p$. Ainsi $\mathcal{M}_0, w_0 \models \neg p$, ce qui est en contradiction avec la définition de v .

(\leftarrow) Supposons que R soit symétrique dans le cadre (W, R) . Soit $\mathcal{M} = (W, R, v)$ un modèle et $w \in W$. Supposons que $\mathcal{M}, w \models p$. Prenons à présent $w' \in R(w)$. Comme $w \in R(w')$, $\mathcal{M}, w' \models \Diamond p$. Ainsi pour tous les $w' \in R(w)$, $\mathcal{M}, w' \models \Diamond p$ et donc $\mathcal{M}, w \models \Box \Diamond p$.

Correction: (Exercice 1.5) Soit t une application transformant une formule modale de K^N en une formule de FO^2 ($i \in \{0, 1\}$):

1. $t(p_j, \mathbf{x}_i) \stackrel{\text{def}}{=} \text{P}_{2 \times j}(\mathbf{x}_i)$;
2. $t(p_j^N, \mathbf{x}_i) \stackrel{\text{def}}{=} \text{P}_{2 \times j+1}(\mathbf{x}_i)$;
3. t est homomorphique pour les connecteurs propositionnels;
4. $t(\Box \phi, \mathbf{x}_i) \stackrel{\text{def}}{=} \forall \mathbf{x}_{1-i} (\text{R}(\mathbf{x}_i, \mathbf{x}_{1-i}) \Rightarrow t(\phi, \mathbf{x}_{1-i}))$.

Soit ϕ une formule modale de K^N avec $\text{For}_0^N(\phi) = \{p_{i_1}^N, \dots, p_{i_n}^N\}$. Soit ψ_ϕ une formule de $\text{FO}^2[=]$ qui exprime que pour $j \in \{i_1, \dots, i_n\}$, $\text{P}_{2 \times j+1}$ est interprété par un singleton, par exemple

$$\bigwedge_{j \in \{i_1, \dots, i_n\}} \exists \mathbf{x}_0 (\text{P}_{2 \times j+1}(\mathbf{x}_0) \wedge \forall \mathbf{x}_1 \neg(\mathbf{x}_0 = \mathbf{x}_1) \Rightarrow \neg \text{P}_{2 \times j+1}(\mathbf{x}_1))$$

Dans le cas où $\text{For}_0^N(\phi) = \emptyset$ on prend $\psi_\phi \stackrel{\text{def}}{=} \top$. On définit alors T de la façon suivante:

$$\text{T}(\phi) \stackrel{\text{def}}{=} \psi_\phi \wedge \exists \mathbf{x}_0 t(\phi, \mathbf{x}_0)$$

Comme pour la proposition 1.10, on peut montrer que ϕ est \mathcal{L} -satisfaisable ssi $\text{T}(\phi)$ est $\text{FO}^2[=]$ -satisfaisable. La réponse à la deuxième question est alors immédiate.

Correction: (Exercice 2.1) By definition $\mathcal{M}, w \models \forall(\phi_1 U \phi_2)$ ssi $\mathcal{M}, w \models \neg \exists G \neg \phi_2 \wedge \neg \exists (\neg \phi_2 U (\neg \phi_1 \wedge \neg \phi_2))$ ssi

1. pour tous les chemins infinis w_0, w_1, \dots avec $w_0 = w$, il existe $k \geq 0$ tel que $\mathcal{M}, w_k \models \phi_2$ et
2. pour tous les chemins infinis w_0, w_1, \dots avec $w_0 = w$, et pour $k \geq 0$, $\mathcal{M}, w_k \models \neg(\neg \phi_1 \wedge \neg \phi_2)$ ou bien il existe $0 \leq i < k$ tel que $\mathcal{M}, w_i \models \phi_2$

ssi pour tous les chemins infinis w_0, w_1, \dots avec $w_0 = w$, il existe $k \geq 0$ tel que $\mathcal{M}, w_k \models \phi_2$ et pour $j \geq 0$, $\mathcal{M}, w_j \models \phi_1 \vee \phi_2$ ou bien il existe $0 \leq i < j$ tel que $\mathcal{M}, w_i \models \phi_2$ ssi pour tous les chemins infinis $w = w_0, w_1, \dots$, il existe $k \geq 0$ tel que $\mathcal{M}, w_k \models \phi_2$ et pour $0 \leq i < k$, $\mathcal{M}, w_i \models \phi_1$.