Étude Bibliographique HAI728I

Spécification et vérification d'un système cyber-physique en logique temporelle

Étudiants

Charlotte Fabre

Gatien Haddad

Référent

Christian Rétoré

Faculté des Sciences

Université de Montpellier

M1 - CMI Informatique - HAI728I

2022-2023

Table des matières

1 Introduction

La logique mathématique, qui étudie notamment les formules propositionnelles et du premier ordre, a donné naissance à de nombreuses branches qui se subdivisent elles-mêmes en logiques plus spécifiques. Ces différents systèmes permettent de modéliser une gamme de problèmes variés, comme des énoncés mathématiques, des problèmes de réseaux de contraintes ou encore des spécifications de systèmes cyber-physiques.

Cette dernière application requiert la prise en compte d'une notion d'écoulement du temps. En effet, les systèmes cyber-physiques sont constitués d'éléments physiques et informatiques collaborant entre eux. En particulier, les objets physiques interagissent relativement les uns aux autres, c'est-à-dire avant ou après les opérations des autres éléments. Un tel concept peut être modélisé par l'utilisation de la logique temporelle, une branche de la logique modale qui ajoute certains opérateurs supplémentaires aux connecteurs de la logique propositionnelle.

Dans le cadre du projet long intégrateur CMI HAI728I, le sujet encadré par M. Christian Rétoré a pour objectif de spécifier et de vérifier un système cyber-physique en logique temporelle. Pour préparer au mieux le travail du semestre prochain, nous avons choisi d'orienter cette synthèse bibliographique sur la définition des logiques modales et temporelles, afin d'avoir une compréhension globale des divers concepts qu'elles introduisent.

Ainsi, nous définirons principalement les logiques modales et temporelles, en première et deuxième partie, en nous attardant pour chacune sur leur syntaxe, leur sémantique et leurs représentations. Nous proposerons également plusieurs exemples détaillés au cours de ce rapport, afin d'appliquer les différents concepts théoriques présentés. Enfin, nous décrirons notre organisation de travail et nos perspectives pour le semestre suivant.

2 Logique modale et modèles de Kripke

2.1 Rappels de logique propositionelle

La logique propositionnelle manipule des formules appelées **propositions** et construites à partir de différents symboles. Tout d'abord, les constantes $\top$ (***Top***, toujours vrai) et $\bot$ (***Bottom***, toujours faux) permettent de représenter les deux valeurs de vérité. À celles-ci, s'ajoute l'ensemble des symboles propositionnels (tels que p, q, r, ...) consitué de variables qui peuvent être interprétées, c'est-à-dire se voir attribuer une valeur parmi « vrai » ou « faux ». Enfin, cinq symboles supplémentaires sont utilisés, afin de construire des propositions plus ou moins complexes. Ce sont les **opérateurs** ou **connecteurs logiques** :

— La négation $\neg$: $\neg p$ est vrai si p est faux
— La conjonction $\wedge$: $p \wedge q$ est vrai si p et q sont tous les deux vrais
— La disjonction $\vee$: $p \vee q$ est vrai si p est vrai, q est vrai, ou les deux le sont
— L'implication $\rightarrow$: $p \rightarrow q$ est vrai si lorsque p est vrai, q l'est également
— L'équivalence $\iff$: $p \iff q$ est vrai si p et q ont la même valeur

Avec ces différents symboles, il est possible de construire des **formules bien formées**, souvent notées ϕ. Par exemple, $p \wedge (q \vee r)$ et $\neg p \iff (q \rightarrow r)$ sont des formules bien formées, et $\neg \wedge p$ n'en est pas une.

2.2 Introduction à la logique modale

2.2.1 Notion d'opérateur de modalité

La logique modale a pour but d'étendre la logique propositionnelle, en introduisant différents **modes** ou **opérateurs de modalités** qui peuvent être unaires ou binaires. Ces opérateurs précisent le contexte de vérité des formules auxquelles ils sont appliqués. Ainsi, une formule n'est pas seulement vraie, mais doit être vraie, peut être vraie, est toujours vraie, est crue vraie, ...

Les modes sont donc nombreux et spécifient différentes qualités du « vrai » logique, mais leur utilisation est sensiblement la même d'une famille de logique modale à l'autre. Deux d'entre eux seront donc définis ici, et cette définition pourra être étendue aux autres modes présentés dans ce rapport. Soit ϕ une formule bien formée, alors deux des modes de la logique modale sont :

— $\Box(\phi)$, qui signifie « il est nécessaire que ϕ ».
— $\Diamond(\phi)$, qui signifie « il est possible que ϕ ».

On peut alors coupler ces opérateurs aux connecteurs de la logique propositionnelle pour former des formules de logique modale.

Soit la formule ϕ : « Il fait beau ». Elle peut être complétée en $\Box(\neg\phi)$, signifiant « Il est nécessaire qu'il ne fasse pas beau », ou en $\neg\Diamond(\phi)$, pour « Il n'est pas possible qu'il fasse beau ».

Les opérateurs de modalité sont liés deux à deux pour former des paires au sein desquelles chaque opérateur peut être défini en fonction de l'autre. Ainsi, $\Box$ et $\Diamond$ peuvent être redéfinis ainsi :

— $\Box(\phi) = \neg\Diamond(\neg\phi)$
— $\Diamond(\phi) = \neg\Box(\neg\Box))$

Les modes sont donc ce qui rassemble les différentes familles de logique modale au sein d'une même logique.

2.2.2 Différentes familles de logique modale

Les différentes familles de logique modale évoquées précédemment, dans lesquelles divers modes sont introduits, sont nombreuses. Certaines d'entre elles sont présentées dans cette partie.

2.2.2.1 Logique déontique

La logique déontique est une des premières logique dérivées de la logique modale. Introduite par Leibniz au XVII^{e} siècle, cette logique ajoute une dimension philosophique de **morale** à la logique propositionnelle. Elle se sert des quatre connecteurs suivants :

- $\boldsymbol{O}$ représente ce qui est obligatoire
- $\boldsymbol{P}$ correspond à ce qui est permis ou juste
- $\boldsymbol{I}$ est utilisé pour ce qui est interdit
- $\boldsymbol{F}$ est ce qui est facultatif

Ainsi, soit ϕ la formule suivante : « Respecter autrui ». Alors, on peut écrire :

- $O\phi$: il est obligatoire de respecter autrui
- $P\phi$: il est permis de respecter autrui
- $I\neg\phi$: il est interdit de ne pas respecter autrui
- $\neg F\phi$: il est n'est pas facultatif de respecter autrui

Dans cet exemple, la notion d'obligation est évoquée par chacune des phrases interprétées en language naturel. Ainsi, comme c'était le cas pour $\Box$ et $\Diamond$, les modalités de la logique déontique peuvent être définies les unes par les autres. Avec O par exemple, les définitions reformulées sont les suivantes :

- $P(\phi) = \neg O(\neg\phi)$
- $I(\phi) = O(\neg\phi)$
- $F(\phi) = \neg O(\phi)$

2.2.2.2 Logique épistémique

Une autre logique appartenant à la famille des logiques modales est la logique épistémique. Dans celle-ci, est introduite la notion de **connaissance** sur un ou plusieurs **agents**. Cette connaissance est représentée par les deux modalités présentées plus tôt : $\Box$ et $\Diamond$. Dans le cadre épistémique cependant, ces deux modes n'ont pas le même sens qu'en logique temporelle :

- $\Box_i(\phi)$ signifie « l'agent i sait que ϕ »
- $\Diamond_i(\phi)$ signifie « l'agent i croit possible que ϕ »

Comme pour les différents modes déjà présentés, les deux opérateurs de modalité de la logique épistémique sont liés par leurs définitions :

- $\Box_i(\phi) = \neg\Diamond_i(\neg\phi)$
- $\Diamond_i(\phi) = \neg\Box_i(\neg\phi)$

À titre d'exemple, soit la formule ϕ : « Il fait beau », ainsi que deux agents Alice et Bob, abrégés en A et B. Les formules $\Box_A(\phi)$ et $\Diamond_B(\neg\Box_A(\phi))$ correspondent respectivement à « Alice sait qu'il fait beau » et « Bob croit possible que Alice ne sache pas qu'il fait beau ».

2.2.2.3 Logique temporelle

La logique modale la plus intéressante pour la modélisation de systèmes cyber-physiques est la **logique temporelle**. Celle-ci introduit différents modes dans le but de nuancer la valeur de vérité par une situation temporelle : une formule donnée a été vraie, pourra être vraie, sera vraie après un évènement, ... La partie Logique temporelle : *Linear Temporal Logic* et *Computation Tree Logic* de ce rapport est entièrement consacrée à cette logique.

La définition des opérateurs de modalités et la présentation de différentes logiques modales a permis de définir le cadre syntaxique dans lequel s'inscrit la logique temporelle. Pour y ajouter de la sémantique, un nouvel élément doit être considéré : le concept de modèle de Kripke.

2.3 Modèles de Kripke

Au XVIII^{e} siècle, le philosophe Leibniz introduit une nouvelle théorie : celle de différents mondes possibles. Sommairement, il s'agit de considérer que plusieurs réalités peuvent exister dans différents mondes, tous possibles. Ainsi, des idées pourraient être vraies dans un monde et fausses dans un autre. D'un point de vue logique, cela se traduirait par le fait que des formules propositionnelles aient une certaine valeur dans un monde donné, et une valeur opposée dans un autre. Cette théorie peut donc être reprise dans le cadre logique : c'est ce que font Saul Kripke, Jaakko Hintikka et Stig Kanger dans les années 1950. Ils développent ainsi une sémantique formelle basée sur le concept de mondes possibles, qui s'impose rapidement en tant que sémantique des formules modales, de par sa puissance mais également grâce à son intuitivité et à la simplicité de sa définition.

2.3.1 Cadre de Kripke

Pour définir formellement la sémantique de Kripke, il est nécessaire d'introduire la notion de **cadre de Kripke**. Les cadres de Kripke sont formés par des couples $(\mathcal{M}, R)$.

- $\mathcal{M}$ est un ensemble **non-vide** de mondes. Le i$^{\text{ème}}$ monde possible est noté : $m_i \in \mathcal{M}$.
- R est une relation binaire sur $\mathcal{M}$, appelée relation d'accessibilité. C'est un sous-ensemble quelconque de $\mathcal{M} \times \mathcal{M}$, ce qui signifie qu'il peut exister des mondes qui ne sont pas en relation. Pour les mondes qui le sont, la relation est écrite : $m_i \mathcal{R} m_j$. Le monde m_j est alors **accessible** depuis le monde m_i.

Ainsi, $(\mathcal{M} = \{m_1, m_2, m_3\},\ \mathcal{R} = \{(m_1, m_1),\ (m_1, m_2),\ (m_1, m_3), (m_2, m_3)\})$ est un cadre de Kripke dans lequel tous les mondes sont accessibles depuis m_1, et aucun n'est accessible depuis m_3.

2.3.2 Construction des modèles de Kripke

Les **modèles de Kripke** sont construits en ajoutant une **fonction de valuation** à un cadre de Kripke. Cette fonction de valuation associe un ou des mondes de $\mathcal{M}$ à une ou des parties P de l'ensemble des propositions $\mathcal{P}$.

En général, la valuation est représentée de trois façons différentes :

- La fonction $h : \mathcal{M} \to P(\mathcal{P})$, alors $h(m_i) = \{\phi, \psi\}$ par exemple
- La fonction $h : P(\mathcal{P}) \to (\mathcal{M})$, alors $h(\phi) = \{m_i, m_j\}$ par exemple
- L'opérateur $\Vdash$, avec lequel les deux exemples précédents s'écrivent respectivement $(\mathcal{M}, m_i \Vdash \phi, \psi)$ et $(m_i \Vdash \phi,\ \mathcal{M}, m_j \Vdash \phi)$. Il faut alors lire $\mathcal{M}, m_i \Vdash \phi$ comme « La formule ϕ est vraie dans le monde m_i du modèle $\mathcal{M}$ ». C'est cette écriture qui sera préférée dans la suite de ce rapport, pour sa simplicité et son expressivité. En effet, elle permet également de préciser

qu'une formule est fausse dans un monde d'un modèle : $\mathcal{M}, m_i \nVdash \phi$. Par souci de clarté et de lisibilité, $\mathcal{M}, m_i \Vdash \phi$ sera écrit $m_i \Vdash \phi$ dans la suite de ce rapport, et il sera alors admis que $m_i \in \mathcal{M}$.

Ainsi, il est possible de construire un modèle de Kripke en ajoutant la fonction de valuation suivante au cadre défini précédemment : $\{m_1 \Vdash \phi; m_2 \Vdash \phi, \psi; m_3 \Vdash \phi\}$. Ce modèle peut être représenté comme le graphe orienté suivant :

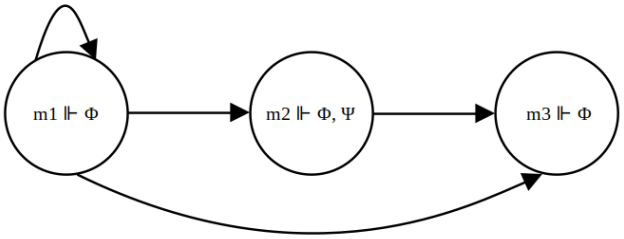


FIGURE 1 – Exemple de modèle de Kripke

Dans ce modèle, la formule ϕ est Kripke-valide, c'est-à-dire qu'elle est vraie dans tous les mondes possibles. La formule ψ, quant à elle, est Kripke-satisfiable, c'est-à-dire qu'elle est vraie dans au moins l'un des mondes possibles.

2.3.3 Sémantique des logiques modales dans les modèles de Kripke

La sémantique des modalités de la logique temporelle dans les modèles de Kripke est la suivante :

— si $m_i \Vdash \Box\phi$, alors pour tout monde m_j **accessible** depuis m_i, $m_j \Vdash \phi$

— si $m_i \Vdash \Diamond\phi$, alors il existe un monde m_j **accessible** depuis m_i tel que $m_j \Vdash \phi$

Dans ces deux définitions, c'est la relation d'accessibilité $\mathcal{R}$ qui donne leur sémantique aux modes. Cependant, les logiques modales sont nombreuses et variées, elles ne peuvent donc pas toutes être représentées à l'aide d'un seul modèle de Kripke.

Pour distinguer les sémantiques de différents modèles, la relation d'accessibilité est alors utilisée : pour associer une sémantique à un modèle de Kripke, il faut définir des propriétés que sa relation $\mathcal{R}$ doit respecter. Chacune de ces propriétés correspond à une formule appelée **Formule de Sahlqvist**. Si celle-ci est vérifiée par la relation d'accessibilité, alors la formule est valide dans le cadre de Kripke associé, et inversement.

Pour illustrer cette équivalence, certaines des propriétés sont les suivantes :

— **Sérialité**

La relation d'accessibilité $\mathcal{R}$ est sérielle s'il existe au moins un monde accessible depuis chacun des mondes de $\mathcal{M}$. La formule de Sahlqvist qui lui est associée est $\Box\phi \rightarrow \Diamond\phi$. En effet, par la sémantique de $\Box$, pour tout monde accessible depuis m_i tel que $m_i \Vdash \Box\phi$, il faut que ϕ soit vrai. Or, par la sérialité de $\mathcal{R}$, il existe au moins un monde m_j accessible depuis m_i. Donc $\Diamond\phi$ est bien vérifiée pour tout monde où $\Box\phi$ l'est.

— **Réflexivité**

$\mathcal{R}$ est réflexive si tout monde est en relation avec lui-même. La formule de Sahlqvist associée est $\Box\phi \rightarrow \phi$. En effet, par la sémantique de $\Box$, pour tout monde accessible depuis m_i tel que $m_i \Vdash \Box\phi$, il faut que ϕ soit vrai. Or, m_i est accessible depuis lui-même, donc ϕ est bien vérifiée pour tout monde où $\Box\phi$ l'est.

— **Transitivité**

La relation d'accessibilité $\mathcal{R}$ est transitive si pour des mondes consécutivement accessibles

l'un par l'autre, le dernier est accessible depuis le premier. La formule de Shalqvist associée à cette propriété est $\Box\phi \rightarrow \Box\Box\phi$. Par transitivité, si m_j est accessible depuis m_i, et m_k depuis m_j, alors m_k est également accessible depuis m_i. Soit $m_i \Vdash \Box\phi$, alors on sait que pour tous les mondes m_j tel que $m_i \mathcal{R} m_j$, $m_j \Vdash \phi$. Comme $\mathcal{R}$ est transitive, on sait qu'il n'existe pas de monde m'_j tel que $m_j \Vdash m'_j \wedge m_i \nVdash m'_j$. Ainsi, puisque tous les mondes accessibles par m_j forcent ϕ (par $m_i \Vdash \Box\phi$), alors tous ces mondes forcent aussi $\Box\phi$. Donc $m_j \Vdash \Box\phi$, et il faut $m_i \Vdash \Box\Box\phi$

2.3.4 Représentation des modèles de Kripke et exemple des *Muddy Children*

Pour avoir une compréhension globale des modèles de Kripke, il est possible de les représenter graphiquement à l'aide de graphes orientés. Les états représentent alors les différents mondes possibles et les arcs montrent l'accessibilité : si $m_a \mathcal{R} m_b$ et A et B les représentent dans le graphe, alors il y a un arc de A vers B.
L'exemple des *Muddy Children*, qui est une énigme étudiée en logique épistémique, va permettre d'illustrer efficacement cette représentation.

2.3.4.1 Présentation du puzzle des *Muddy Children*

L'énoncé de l'énigme est le suivant :

> Un père laisse ses n enfants jouer dans un jardin boueux en leur demandant à tous d'éviter de se salir. Lorsque les enfants rentrent, certains ont de la boue sur le front. Chacun d'entre eux ne peut pas savoir s'il est sale ou non, puisqu'il n'a pas pu communiquer avec ses frères et soeurs, mais il peut voir qui est sale parmi les autres enfants. Lorsqu'il les voit, le père mécontent leur dit : « Au moins l'un d'entre vous est sale. Si l'un d'entre vous sait qu'il est sale, qu'il lève la main. », et il répète cette phrase tant qu'aucun enfant n'a levé la main.

Le but de ce problème est de comprendre que s'il y a n enfants sales, tous lèveront la main au bout de la n-ième répétition. Les mondes de Kripke sont l'outil le plus efficace pour arriver à une telle conclusion.

2.3.4.2 Construction du modèle de Kripke pour deux enfants

Dans le cas où $n = 2$, soient Alice et Bob les deux enfants et S_i la formule « Le front de i est sale ».
Le fait qu'Alice voie le front de Bob peut être traduit par $\Box_A S_B$ si Bob est sale, et $\Box_A \neg S_B$ sinon. Ces formules se lisent « Alice sait que Bob est sale » et « Alice sait que Bob n'est pas sale », et elles sont analogues du point de vue de Bob.

Quatre configurations différentes de cet énoncé peuvent alors exister. Pour les représenter, il s'agit dans un premier temps de définir un cadre de Kripke dans lequel $\mathcal{M} = \{m_1, m_2, m_3, m_4\}$. Dans le cadre de la logique épistémique, la relation binaire $\mathcal{R}$ est remplacée par $\equiv_i$, qui est la relation d'accessibilité pour l'agent i : $m_i \equiv_A m_j$ si Alice peut considérer m_j depuis m_i.
Pour construire un modèle de Kripke à partir de ce modèle, il faut y ajouter une fonction de valuation. En logique épistémique, cette fonction est le *forcing atomique* $\Vdash$ entre un monde m_i et une formule ϕ : $m_i \Vdash \phi$, qui se lit m_i force ϕ.

2.3.4.3 Résolution du problème pour deux enfants

Pour le problème des deux enfants sales, les quatre mondes peuvent être représentés visuellement comme ceci :

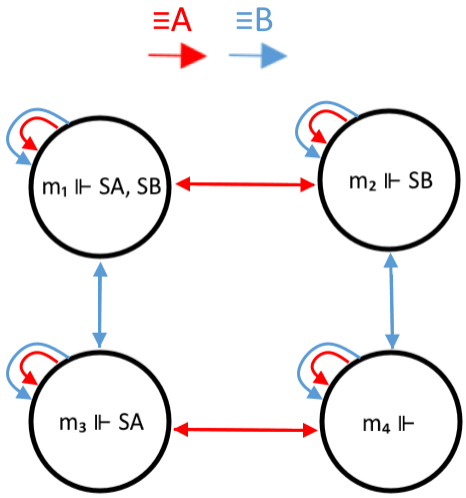


FIGURE 2 – Mondes de Kripke du problème des *Muddy Children* pour le cas de deux enfants

Cette première illustration met en valeur plusieurs informations. Tout d'abord, la relation d'accessibilité entre les mondes est réflexive : $\forall m \; \forall i \; m \equiv_i m$. Ensuite, pour Alice, les mondes accessibles dépendent du monde dans lequel elle se trouve réellement. Si la situation réelle est celle du monde m_1, Alice et Bob sont tous deux sales. Depuis ce monde, Alice voit donc que Bob est sale ($\Box_A S_B$) et inversement ($\Box_B S_A$). Par la relation d'accessibilité $\equiv_A$, Alice peut atteindre les mondes m_1 et m_2. Or, puisqu'elle sait que Bob est sale, elle sait également que le monde réel est celui dans lequel tous deux sont sales, ou celui où seul Bob l'est. Elle n'envisage pas que Bob ne soit pas sale, car elle sait qu'il l'est. Les informations tirées permettent donc de conclure que si Alice se trouve dans le monde m_1, elle considère les mondes m_1 et m_2 : $m_1 \Vdash \Diamond_A S_A$.

Pour revenir au problème initial, en disant « Au moins l'un d'entre vous est sale », le père donne une information aux enfants. En effet, Alice et Bob savent tous les deux que le monde m_4 n'est pas envisageable, puisque $m_4 \Vdash \neg S_A \wedge \neg S_B$. En raisonnant à l'aide des mondes de Kripke, Alice se rend alors compte qu'il ne reste que deux possibilités :

— Elle est dans le monde m_1 et elle est donc sale. Bob considère alors les mondes m_1 et m_3, et lui non plus ne peut pas savoir s'il est sale ou non.
— Elle est dans le monde m_2 et elle n'est donc pas sale. Bob ne considère alors plus que le monde m_2 et il peut savoir qu'il est sale.

Lorsque le père ajoute « Si l'un de vous sait qu'il est sale, qu'il lève la main », aucun des deux enfants ne peut lever la main : ils ne savent pas s'ils sont eux-mêmes sales ou non, à cause de $\Diamond_A S_A = \neg\Box_A\neg S_A$. Dès lors, Alice acquiert la connaissance que Bob ne sait pas s'il est sale ou pas : $\Box_A\Diamond_B S_B$. Elle peut donc éliminer le monde m_2, car $m_2 \Vdash \Box_B(S_B)$. Alice ne considère donc plus que le monde m_1, et comme $m_1 \Vdash S_A$, lorsque le père répète sa phrase aux enfants, Alice lève la main. Tout ce raisonnement peut être reproduit pour Bob.

Couplé à la définition des logiques modales, la présentation des mondes de Kripke permet de poser un cadre clair et concret pour la définition de la logique temporelle.

3 Logique temporelle : *Linear Temporal Logic* et *Computation Tree Logic*

3.1 Introduction à la logique temporelle

La logique temporelle est une logique modale dont l'une des principales utilisations est la vérification et/ou **spécification formelle** de programmes.
Étant une des logiques modales, elle reprend les différents éléments syntaxiques vus dans la section précédente : des symboles propositionnels, des connecteurs logiques et des opérateurs de modalité. Les modes spécifiques à la logique temporelle seront introduits un peu plus tard dans cette section. Les symboles propositionnels utilisés en logique temporelle, quant à eux, peuvent être de l'un des deux types suivants :

- Les variables propositionnelles $p, q, r, ...$, qui sont utilisées de la même façon que dans la logique propositionnelle
- Les variables de type t_i et n_i, représentant respectivement l'i$^{\text{ème}}$ moment de temps et l'i$^{\text{ème}}$ intervalle de temps, et qui permettent d'indiquer dans quel temps une modalité est utilisée.

Pour représenter le temps sous ses différentes formes, la logique temporelle se sépare en deux sous-branches :

- La **logique en temps linéaire**, ou *Linear Temporal Logic* (LTL), qui représente le temps comme une ligne sur laquelle des évènements se succèdent
- La **logique en temps arborescent**, ou *Computable Tree Logic* (CTL), qui représente le temps comme un arbre dans lequel chaque évènement peut entraîner un embranchement vers plusieurs évènements possibles

Ces deux branches sont représentées dans des sytèmes appelés **systèmes de transition**, qui ressemblent aux graphes orientés utilisés pour illustrer graphiquement les mondes de Kripke. Ils prennent chacun une forme définie : une ligne, ou un arbre.
Dans ces deux branches cependant, les modalités utilisées sont différentes et l'inteprétation des formules est adaptée à la représentation du temps. Ainsi, une valeur de vérité est associée à une suite de parties de $\mathcal{P}$ en LTL, et à un arbre sur une partie de $\mathcal{P}$ en CTL.
Ces deux sous-branches ne sont donc pas équivalentes, et ne permettent pas de représenter les mêmes formules. Pour traiter la logique formelle, il s'agira donc de présenter LTL dans une première partie, et de définir CTL dans une seconde partie.

3.2 *Linear Temporal Logic* (LTL)

La première des deux branches de la logique temporelle est la LTL, ou *Linear Temporal Logic*. Elle permet d'écrire des formules avec une portée lointaine dans le temps : une formule donnée sera par exemple vraie à un temps futur donné.
Pour utiliser la LTL, il faut d'abord présenter les modalités supplémentaires qu'elle utilise.

3.2.1 Introduction à la LTL, définition et modalités supplémentaires

En LTL, les modalités $\Box$ et $\Diamond$ sont utilisées telles qu'elles ont été présentées dans la section précédente. À celles-ci, s'ajoute une certain nombre d'autres modes appelés **opérateurs temporels**. Pour définir ces opérateurs, il faut d'abord présenter différents concepts spécifiques à la logique temporelle linéaire.
Une séquence $S = s_0, s_1, ..., s_n$ est constituée d'un ensemble de n éléments s_i consécutifs appelés

états : elle peut être vue comme un chemin de Kripke dans lequel les mondes sont remplacés par les états. Pour former une interprétation linéaire, une séquence infinie est couplée à une fonction f associant chaque état aux formules qui sont vraies dedans.
Soit s_i un état quelconque d'une intertprétation linéaire, et ϕ et ψ deux formules bien formées, les opérateurs temporels sont les suivants :

- L'opérateur unaire « suivant » $\boldsymbol{X}$ (pour *neXt*) : $s_i \Vdash X\phi$ est vrai si $s_{i+1} \Vdash \phi$, donc $X\phi$ est vrai dans un état si ϕ est vrai à l'état suivant.
- L'opérateur binaire « jusqu'à » $\boldsymbol{U}$ (pour *Until*) : $s_i \Vdash \phi U \psi$ est vrai s'il existe un état s_j tel que $i \leq j$, et tous les états de s_i à s_{j-1} rendent vrai ϕ, puis $s_j \Vdash \psi$.
- L'opérateur binaire « faible jusqu'à » $\boldsymbol{W}$ (pour *Weak until*) : $s_i \Vdash \phi W \psi$ est vrai soit si $s_i \Vdash \phi U \psi$, c'est-à-dire que ϕ est vrai jusqu'à ce que ψ le soit, soit si ϕ est toujours vrai. Avec W, il est donc possible que ψ n'arrive jamais et que la formule reste vraie, ce qui n'était pas le cas avec U.

Pour simplifier l'écriture de formules complexes, certains opérateurs supplémentaires sont parfois ajoutés :

- L'opérateur unaire « globalement » $\mathbf{G}$ (pour *Globally*) : $s_i \Vdash G\phi$ si ϕ est vrai dans l'ensemble des états d'indice supérieur à i. Cet opérateur est équivalent à $\Box\phi$, puisque les états postérieurs à s_i seraient ceux qui sont accessibles depuis s_i dans un modèle de Kripke, est ϕ doit donc être vrai dans ceux-là.
- L'opérateur unaire « finalement » $\mathbf{F}$ (pour *Finally*) : $s_i \Vdash F\phi$ si ϕ est vrai dans au moins l'un des états d'indice supérieur à i. Cet opérateur est équivalent à $\Diamond\phi$.
- L'opérateur binaire « libération » $\mathbf{R}$ (pour *Release*) : $s_i \Vdash \phi R \psi$ si ψ reste vrai au moins jusqu'à ce que ϕ soit vrai. Il doit donc exister un état s_j avec $j \geq i$ tel que $s_j \Vdash \phi, \psi$.

Ces derniers opérateurs ne sont pas primordiaux, car comme pour les autres modalités, ils peuvent être redéfinis :

- $s_i \Vdash G\phi$ si et seulement si $s_i \Vdash \bot R\phi$, c'est-à-dire que ϕ reste toujours vrai.
- $s_i \Vdash F\phi$ si et seulement si $s_i \Vdash \top U\phi$, c'est-à-dire que ϕ devient éventuellement vrai.
- $s_i \Vdash \phi R\psi$ si et seulement si $s_i \Vdash \neg(\neg\phi U \neg\psi)$ ou $s_i \Vdash \psi W(\psi \wedge \phi)$

3.2.2 Exemple de modélisation d'un système en LTL : le passage à niveau

La situation du passage à niveau est adaptée à la modélisation en LTL, puisqu'elle est constituée d'une suite d'évènements consécutifs.
Soient les trois variables propositionnelles suivantes :

- Un train approche : **a**
- Un train passe : **p**
- La barrière est baissée : **b**

Pour modéliser la situation, plusieurs formules peuvent être écrites en LTL :

- « À s_0, la barrière est levée jusqu'à ce qu'un train approche éventuellement » : $s_0 \Vdash \neg b W a$
- « Quand un train approche, il est certain que le train passera » : $\Box(a \rightarrow \Diamond p)$
- « La barrière est baissée jusqu'à ce que le train passe » : $\Box(a \rightarrow pRb)$
- « La barrière se relève juste après que le train soit passé » : $\Box(p \rightarrow X\neg b)$

Une interprétation linéaire satisfaisant toutes ces formules de LTL pourrait être représentée comme ceci :

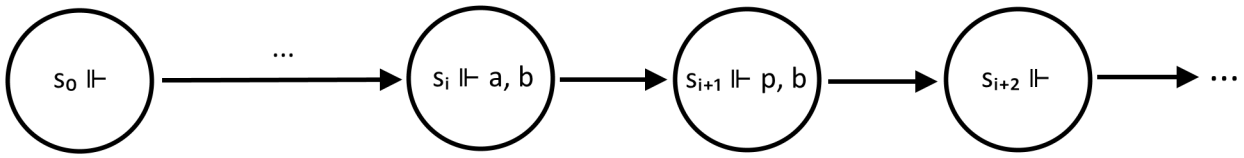


FIGURE 3 – Interprétation linéaire du fonctionnement d'un passage à niveau

3.3 *Computation Temporal Logic* (CTL)

Une seconde branche de la logique temporelle est la CTL, ou *Computation Tree Logic*. Elle permet de considérer différents futurs qui pourraient advenir, sans pour autant savoir lequel représente le futur réel. Pour utiliser la CTL, il faut d'abord présenter les modalités supplémentaires qu'elle utilise.

3.3.1 Introduction à la CTL, définition et modalités supplémentaires

La CTL est la plus forte des deux branches de la logique temporelle, puisque toutes les formules qui peuvent être représentées en LTL peuvent également l'être en CTL. En effet, les lignes de temps représentées en LTL peuvent être vues comme des branches sans ramifications ou chemins détachées d'un arbre en CTL. Cette logique introduit donc une notion de point de choix qui n'existait pas dans le cadre linéaire. Un point de choix est un état à partir duquel plusieurs ramifications sont créées : un état point de choix a plusieurs successeurs.
Pour représenter les formules branchantes, la CTL utilise deux types de modalités qui doivent être combinées :

- Les opérateurs de chemin (*path-specific*) sont repris de la LTL, ce sont X, U, W, G, F et R qui concernent les états d'une même branche.
- Les opérateurs outre-chemin (*over path*) sont introduits dans la CTL, ce sont des préfixes modaux. Ils concernent l'ensemble des ramifications à partir d'un point de choix et sont au nombre de deux :
  - Le préfixe modal **A** signifie que l'opérateur temporel qui le suit doit être vrai dans tous les successeurs de l'état.
    Par exemple, si $AX\phi$ est vraie dans un état, tous les successeurs de cet état doivent vérifier ϕ.
  - Le préfixe modal **E** signifie que l'opérateur temporel qui le suit doit être vrai dans au moins l'un des successeurs de l'état.
    Par exemple, si la formule $EG(\phi)$ est vraie dans un état, au moins l'un de ses successeurs est le premier état d'un chemin au cours duquel ϕ est toujours vrai.

Tout comme les autres modalités, ces deux préfixes modaux spécifiques peuvent être redéfinis l'un par rapport à l'autre. Soit ϕ une formule propositionnelle précédée d'un des opérateurs temporels de CTL :

- $A\phi = \neg E \neg \phi$
- $E\phi = \neg A \neg \phi$

3.3.2 Exemple de modélisation d'un système en CTL : la télécommande

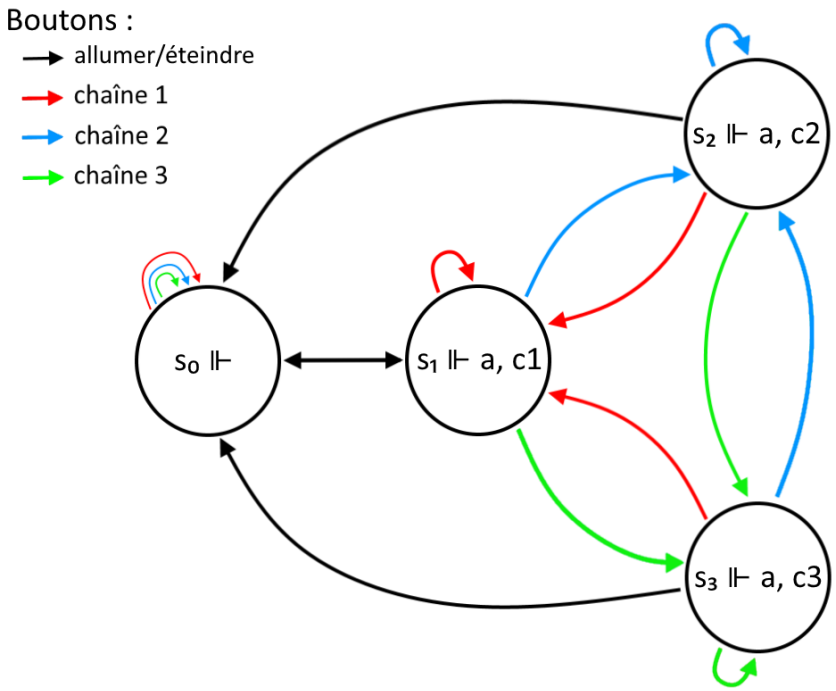
Le système de fonctionnement d'une télécommande permet d'illustrer le concept de temps branchant, puisqu'il propose plusieurs choix à chaque instant de temps. Soient les quatre variables propositionnelles suivantes :

— La télévision est allumée : **a**
— La télévision est réglée sur la chaîne 1 : **c1**
— La télévision est réglée sur la chaîne 2 : **c2**
— La télévision est réglée sur la chaîne 3 : **c3**

Considérons alors les quatre états suivants :

— s_0 : la télévision est éteinte
— s_1 : la télévision est allumée sur la chaîne 1
— s_2 : la télévision est allumée sur la chaîne 2
— s_3 : la télévision est allumée sur la chaîne 3

On peut alors donner un système de transition pour représenter les différents états de la télécommande :



Plusieurs formules de la CTL peuvent alors être déduites de ce système de transition :

— Si la télévision est allumée, alors c'est sur la chaîne 1, 2 ou 3 : $\Box(a \rightarrow (c1 \vee c2 \vee c3))$
— La télévision peut être éteinte depuis n'importe quelle branche de s_0 : $s_0 \Vdash A\Diamond(X\neg a)$
— Si la télévision n'est pas allumée, il n'est pas possible d'accéder à la chaîne 3 : $s_0 \Vdash A\neg Xc3$
— Il existe une branche de s_3 dans laquelle une chaine est toujours allumée avant que la télévision ne soit éteinte : $s_3 \Vdash E((c1 \vee c2 \vee c3)U\neg a)$

4 Travail de groupe : organisation et perspectives futures

4.1 Organisation du travail de groupe

La rédaction de cette synthèse bibliographique a demandé une certaine organisation de groupe que nous allons présenter dans cette partie.
Après avoir choisi de travailler avec M. Rétoré sur le sujet « Spécification et vérification d'un système cyber-physique en logique temporelle », nous avons organisé une première réunion avec notre encadrant. Cela nous a permis de réunir les différents documents à étudier pour construire une synthèse bibliographique complète et cohérente.

Pour travailler et communiquer régulièrement, nous avons mis en place des réunions de groupe hebdomadaires, au cours desquelles nous pouvions partager nos avancées en terme de lecture et de compréhension. Après avoir chacun lu les différents documents à notre disposition, nous avons pu organiser une nouvelle réunion avec M. Rétoré, afin de discuter d'un plan qui permettrait d'organiser au mieux le contenu dans le rapport.
À la suite de cette réunion encadrée, nous avons réalisé que les différents concepts à présenter étaient interdépendants, et qu'il était donc complexe de diviser le travail de rédaction en parties séparées. Nous avons donc passé de nombreuses réunions à subdiviser les parties de ce rapport ensemble, afin d'être sûrs d'éviter les répétitions ou d'oublier du contenu. Nous avons profité de cette période de travail commun pour fixer différents éléments de rédaction, afin de proposer un travail harmonieux : nomenclatures des variables et fonctions, utilisation des titres et sous-titres, ... C'est seulement après ces différentes étapes que nous avons pu commencer à rédiger.

4.2 Bilan et perspectives pour le semestre prochain

La rédaction de cette synthèse bibliographique nous a permis de rassembler de nombreux éléments qui préfacent le travail à venir pour le semestre prochain.
En effet, nous comprenons désormais les différents concepts introduits par les logiques modales, et plus spécifiquement par la logique temporelle. Nous avons ainsi étudié la syntaxe et la sémantique des opérateurs temporels, et appris à les utiliser dans des formules ou à les illustrer dans des systèmes de transition.
Pour le semestre prochain, nous allons donc pouvoir utiliser ces connaissances pour construire la spécification du modèle cyber-physique choisi par notre encadrant : un ascenseur.
Puisque nous nous sommes majoritairement concentrés sur la découverte de la logique temporelle au cours de cette première partie du TER, les notions de spécification et de vérification n'ont pas été abordées.
Au semestre prochain, notre travail constituera donc dans un premier temps à comprendre comment faire une spécification formelle d'un système, et dans un second, à apprendre à vérifier les différentes spécifications produites.

5 Bibliographie

[1] Christian RETORÉ DAVIDE CATTA. "Les bases de la logique modale". 2021.

[2] Jacques DUPARC. *La logique pas à pas*. Chapitre II, Logique Modale. 2015.

[3] Y. Moses R. FAGIN J.Y. Halpern et M.Y. VARDI. "Muddy children puzzle". In : *Reasoning about knowledge* (1995).

[4] John Edensor LITTLEWOOD. "unfaithtful wifes". In : *A mathematician's miscellany* (1953).

[5] Bryan Renne BALTAG Alexandru. *Dynamic Epistemic Logic*. 2016. URL : https://plato.stanford.edu/archives/win2016/entries/dynamic-epistemic/.

[6] WIKIPEDIA. *Kripke semantics*. http://en.wikipedia.org/w/index.php?title=Kripke%20semantics&oldid=1126301019. 2022.

[7] Aurélien LAMERCERIE. *Principe de transduction sémantique pour l'application de théories d'interfaces sur des documents de spécification*. 2021.

[8] WIKIPEDIA. *Temporal logic*. http://en.wikipedia.org/w/index.php?title=Temporal%20logic&oldid=1126312577. 2022.

[9] James GARSON. *Modal Logic*. 2000. URL : https://plato.stanford.edu/entries/logic-modal/.

[10] WIKIPEDIA. *Computation tree logic*. http://en.wikipedia.org/w/index.php?title=Computation%20tree%20logic&oldid=1113052654. 2022.