Mini Mémoire
Le Model-Checking de CTL

BUI QUANG PHUONG Linh – 000427796
Promoteur : Prof. GEERAERTS Gilles

Université Libre de Bruxelles

Résumé La vérification de modèles, plus communément appelée via son appellation anglaise *Model-Checking*, est un système de vérification automatique qu'un système informatique ou électronique satisfasse une certaine propriété. Celle-ci est généralement utilisé afin de prouver la bonne fonctionnalité du système ou dans le cas contraire, de détecter des bugs ou des dysfonctionnements. Plusieurs types d'algorithmes et de logiques permettent d'effectuer un Model-Checking. Nous allons principalement nous intéresser au Model-Checking de CTL mis en place durant les années 80.

Table des matières

1 Introduction

1.1 Contexte et point de vue global

Les dernières décennies entrainant l'évolution exponentielle de la technologie et de l'informatique, la société actuelle fait régulièrement usage de systèmes automatisés afin d'assurer le bon fonctionnement et la fiabilité des programmes, machines et autres divers systèmes informatiques. Afin de vérifier ces systèmes, l'utilisation d'une technique algorithmique appelée *Model-Checking* va être mise en place.
Le principe de base du model-checking est la vérification qu'un certain système satisfasse une certaine propriété. Le système sera représenté par un modèle M tandis que la propriété fera office d'une formule Φ. Dans un premier temps, la modélisation du comportement dynamique du système est nécessaire avant d'être suivie par la vérification de la formule de la propriété grâce à l'algorithme de model-checking qui déterminera si le modèle satisfait bien la formule.

$$\boxed{M \vDash \Phi}$$

Lorsque le système ne satisfait pas la propriété évaluée, le model-checking a donc repéré un bug ou un dysfonctionnement. Chaque année, le coût des bugs s'élève à environ 59 milliards de dollars [6] rien qu'aux Etats-Unis. La création et la mise en place de technique de vérification est donc impérative pour réduire le taux de bugs afin de minimiser ces coûts.

Illustrons cela par un exemple plus concret : un distributeur de boissons. Dans ce cas, il est indispensable que le montant demandé pour une certaine boisson soit mis dans la machine afin que le client puisse récupérer la boisson. La vérification de ce prérequis va être effectué à l'aide d'un système de model-checking. Un autre exemple illustrant l'importance du model-checking est la fermeture des barrières sur une voie ferrée lors du passage d'un train. Celle-ci doit être réalisée automatiquement lorsqu'un train est sur le point de traverser une voie ferrée. Dans ce cas, une petite erreur de timing peut avoir une très grande ampleur concernant la sécurité des passants. Il est donc impératif de vérifier la bonne fonctionnalité du système gérant la fermeture des barrières grâce au model-checking.

1.2 Les phases du model-checking

Le processus de base d'un model-checking est divisé en 3 phases :

1. **La phase de modélisation** : permet de représenter le comportement du système. Dans le cas du model-checking, cette phase de modélisation est réalisée à l'aide d'automates d'états finis et de logique temporelle. Celle-ci permet une formalisation du système ainsi que de la propriété à vérifier. De plus, cette modélisation permet de réaliser les premières vérifications grâce à différentes simulations réalisées sur le modèle. Cette phase de modélisation est l'objet de la section 2 *"Point de vue algorithmique"*.
2. **La phase d'exécution** : exécution du model-checker vérifiant la validité de la propriété à satisfaire.
3. **La phase d'analyse** : lorsque les résultats sont obtenus après exécution, différents cas potentiels existent :
   — Si la propriété est **satisfaite** : vérification de la propriété suivante (si il y en a).
   — Si la propriété n'est **pas satisfaite** : soit un contre-exemple est produit qui décrit un scénario possible d'erreur (violation de la propriété), soit il y a correction du modèle et réexécution du model-checker, soit il y a réexécution de toute la procédure.
   — **Manque de mémoire** (cfr. *State explosion problem*[1]) : tentative de réduction du modèle notamment grâce aux diagrammes de décision binaire ou une réduction partielle de la commande et réexécution le model-checker.

1. Section 1.3 - 1er désavantage

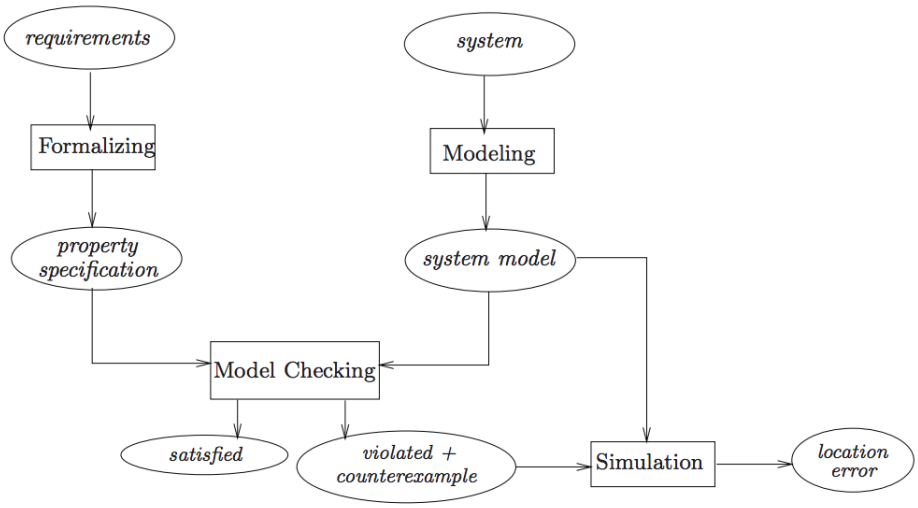

FIGURE 1. Vue schématique de l'approche du model-checking [2]

1.3 Avantages & désavantages

Dans cette section, plusieurs avantages et inconvénients seront présentés sur base des recherches effectuées en 2008 par *Clarke* [3] ainsi que du livre de référence "Principles of Model Checking" [1].

Avantages du model-checking Un model-checking possède plusieurs avantages par rapport à l'utilisation d'éventuelles autres techniques de vérifications et de détection d'erreur. Voici une liste non exhaustive de ces avantages :

- Il s'agit d'une approche générale de vérification applicable dans tous les domaines tels que les systèmes embarqués ou ingénierie logicielle.
- La phase de vérification est automatique. Suivant la phase de modélisation, la seule action nécessaire de l'utilisateur afin de faire fonctionner le model-checking est de l'activer. Le programme s'occupe du reste. Niveau performance, cet automatisme permet un gain de temps conséquent.
- Contrairement aux simples tests, le model-checking va également prouver la bonne fonctionnalité du système et dans le cas contraire, nous renvoyer un contre-exemple d'une exécution du système qui falsifie la propriété et ainsi, détecter le(s) bug(s). Le taux d'erreurs non repérés est donc moindre par rapport aux tests simples.
- Le model-checking agit sur tout le système et non qu'une seule partie, il s'agit donc d'une méthode exhaustive. Néanmoins, si l'utilisateur le souhaite, il est tout de même possible d'utiliser le model-checking pour une vérification partielle et ainsi l'appliquer à des parties de système.
- Utilisation de la logique temporelle (*cfr. section 3.1 "Logique temporelle"*) qui permet d'exprimer facilement les diverses propriétés.

Désavantages du model-checking Néanmoins, le model-checking est une solution discutable sur certains points :

- Le model-checking grandit exponentiellement au nombre de processus actifs (appelés états, correspondant à la taille du système). Pour N variables avec un domaine de k valeurs possibles, le nombre d'états grandit de k^N. Par exemple, pour 20 variables booléennes, il y aurait déjà 2^{20} soit 1048576 états. Le modèle devient donc très vite surchargé et surpasse la

2. Source : Christel Baier and Joost-Pieter Katoen, Principles of Model Checking [1], p.8 figure 1.4

capacité de la mémoire. Ce problème est appelé *State explosion problem* [4]. Par conséquent, le model-checking ne pourrait donc pas croître. Cependant, plusieurs recherches ont été établies dans le but d'établir une solution à ce problème tels que les *diagrammes de décisions binaires* permettant de représenter plusieurs états en un diagramme.

— Le model-checking s'applique généralement sur des systèmes finis et n'est pas adapté aux systèmes non-finis de part sa modélisation grâce à des automates d'états finis. Hors, la possibilité de tomber sur un système non-fini (ayant donc une infinité de valeurs possibles pour les variables) n'est pas écartée.
— Comme son nom l'indique, le model-checking exécute une vérification du modèle du système et non du système en lui-même. Les résultats obtenus pour le modèle correspondent en grande partie au système réel, néanmoins, il est nécessaire d'utiliser des techniques supplémentaires comme des tests pour trouver les éléments qui pourraient différer entre le modèle et le système réel, que ce soit au niveau du hardware tel que des défauts de fabrication ou bien au niveau software tel que des erreurs de codage.
— Conséquence du dernier point : le résultat n'est donc pas garanti à 100% et pourrait donc contenir des erreurs.

2 Point de vue algorithmique

2.1 Graphes et principes d'états

Le model-checking base sa représentation sur un système de graphe orienté, plus précisément sur un *système d'états finis* où chaque noeud du graphe est appelé état tel que les arcs entre ces états sont appelés transitions. Cet ensemble d'états et de transitions décrit le comportement du système réactif et forme le **modèle** de ce système.

Dans l'exemple du problème de distributeur de boissons abordé précédemment, un tel modèle se présenterait comme tel :

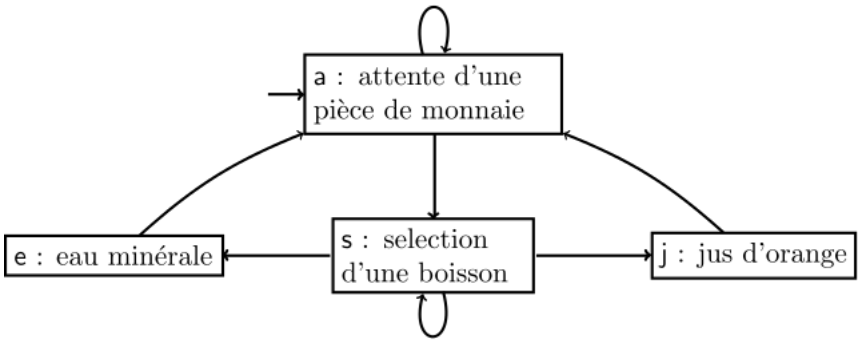

Figure 2. Modèle du problème d'un distributeur de boissons [3]

où chaque état est définie par un nom (un alias). Par exemple, "a" définit l'attente de l'entrée d'une pièce de monnaie dans la machine.

Un modèle de ce type suit la **structure de Kripke** et est donc appelé *modèle de Kripke*.

3. Source : Wikipedia, "Vérifications de modèles"

2.2 Structure de Kripke

Définition *Kripke* définit sa structure, donnant nom à la structure de Kripke [7] :

$$\boxed{K = (S, I, A, AP, \delta, \lambda)}$$

tel que :

- **S** est un ensemble fini d'états,
- $\boldsymbol{I \subseteq S}$ est l'ensemble des états initiaux,
- **A** est un ensemble d'actions,
- **AP** est un ensemble de propositions atomiques,
- $\boldsymbol{\delta \subseteq S \times A \times S}$ est une relation de transitions entre états,
- $\boldsymbol{\lambda : S \rightarrow 2^{AP}}$ est une fonction de labelisation (étiquetage) des états qui fait correspondre chaque état avec la proposition qui y est liée.

Exemple complet d'une structure de Kripke Toujours sur base du même problème de distributeur de boissons, le modèle de la Figure 2 peut-être repris et complété en se voyant attribuer des noms d'actions afin de pouvoir spécifier les transitions et par conséquent de respecter la structure de Kripke.

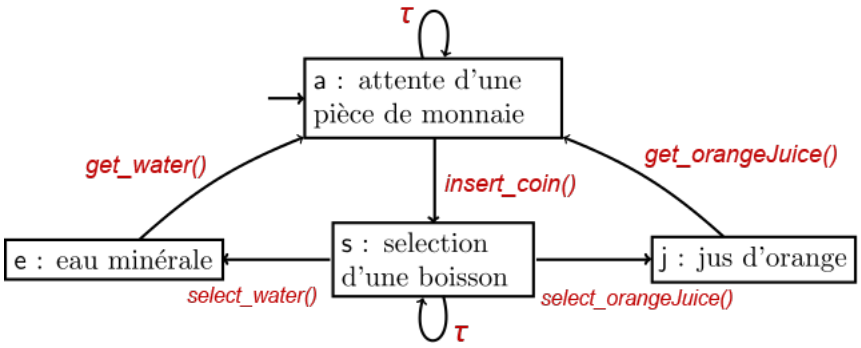

Figure 3. Modèle de Kripke complet du problème d'un distributeur de boissons

Dans ce cas, l'ensemble d'états est $S = \{a, e, s, j\}$. L'ensemble d'états initiaux $I = \{a\}$ ici ne comporte qu'un seul état initial et est représenté dans le modèle par un arc d'entrée vers l'état initial a.

Les labels associés à chaque transition correspond à une action et fait donc partie de l'ensemble d'action A. Le symbole τ représente une action qui n'est pas particulièrement intéressant à étiquetter mais qui n'est néanmoins pas à négliger tels que l'attente de la pièce ou une non-sélection de boisson. L'ensemble d'action est donc $A = \{select\_water, select\_orangeJuice, insert\_coin, get\_orangeJuice, \tau\}$.

Les états et actions maintenant définies, des exemples de relations de transitions peuvent être présentés. Voici les transitions d'états lors de l'achat d'un jus d'orange dans le distributeur :

1. $\boldsymbol{\delta(a, insert\_coin, s)}$: représente la transition de l'état *attente d'une pièce de monnaie* à l'état *sélection d'une boisson* grâce à l'action d'insertion de pièce *insert_coin*.
2. $\boldsymbol{\delta(s, select\_orangeJuice, j)}$: représente la transition de l'état *sélection d'une boisson* à l'état *jus d'orange* grâce à l'action *select_orangeJuice*.

3. $\boldsymbol{\delta(j, get\_orangeJuice, a)}$: représente la transition de l'état *jus d'orange* à l'état *attente d'une pièce de monnaie* grâce à l'action *get_ orangeJuice*.

Ces 3 exemples de transitions font partie des 7 transitions d'états possibles du modèle.

Finalement, concernant le choix des propositions atomiques, le choix le plus simple est d'utiliser le nom des états comme propositions atomiques.
La fonction de labelisation serait donc $\lambda(s) = \{s\} \forall s \in S$.

2.3 Arbre d'exécution d'une structure de Kripke

Définition Un *arbre d'exécution d'une struture de Kripke* correspond au "dépliage" du modèle de Kripke où les noeuds correspondent aux états tel que la racine est l'état initial du modèle de Kripke. Au niveau i, les fils d'un noeud sont les états successeurs au niveau i+1, c'est-à-dire les états subissant une transition à partir du noeud du niveau i.

Pourquoi utiliser un arbre ? L'utilisation d'un arbre permet de représenter tous les chemins de la structure de Kripke. Lorsque le graphe de Kripke est cyclique, l'arbre résultant est un arbre infini. C'est notamment de cette transformation en arbre que le model checking CTL (Computation Tree Logic) tient son nom vu qu'il se base sur la structure en arbre du système.

Illustration : d'un graphe à un arbre. Afin d'illustrer la transformation de la structure de Kripke à un arbre, reprenons une nouvelle fois l'exemple du distributeur de boissons dont le modèle de Kripke est présentée à la Figure 3 et transformons celui-ci en arbre.

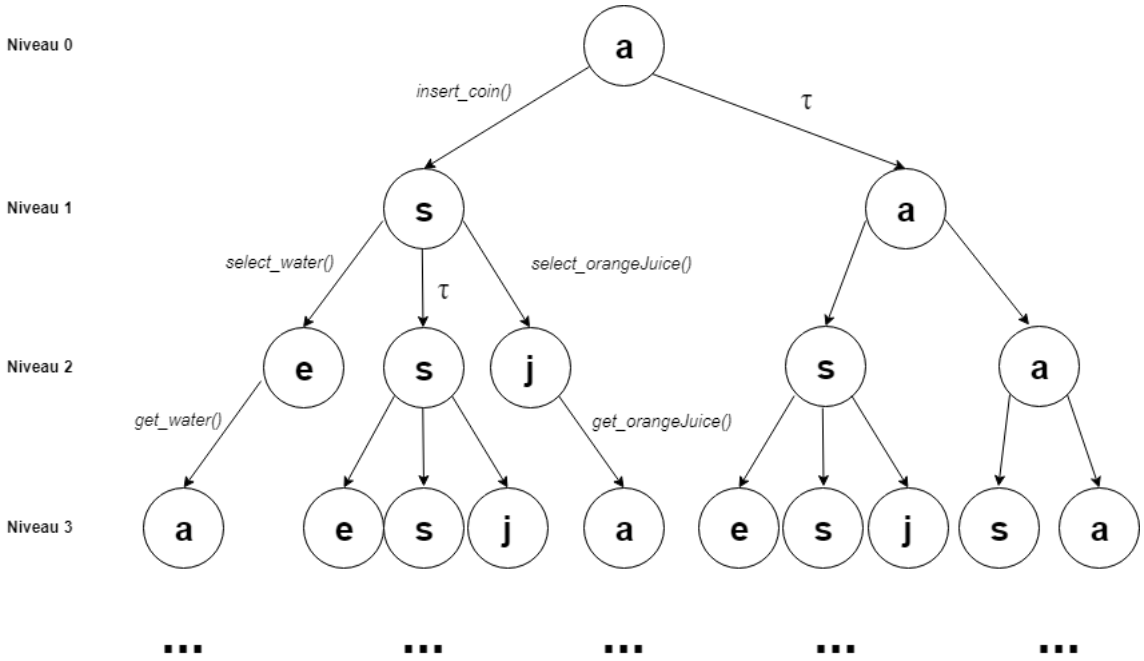

Figure 4. Arbre du problème d'un distributeur de boissons

Tous les éléments présents dans le modèle de Kripke se retrouvent bien dans l'arbre. Dans ce cas, il s'agit bien d'un arbre infini résultant d'un graphe cyclique dont les 4 premiers niveaux sont présentés dans la Figure 4. Le niveau 0 représente la racine de l'arbre.

3 Le model-checking de CTL : généralités et logiques

3.1 Introduction à la logique temporelle

Première approche de la notion de logique temporelle, des différentes sortes de logiques temporelles existantes (linéaire ou arborescente), des propositions de logiques temporelles, des formules associés, ...

LTL Aperçu et premier approche de la logique temporelle linéaire LTL

CTL Aperçu et premier approche de la logique temporelle linéaire CTL

3.2 Avantages d'une structure d'arbre

Présentation des différents avantages de CTL

Brève comparaison avec LTL Comparaison (avantages+désavantages) par rapport à LTL

Exemple d'arbre CTL Exemple d'un arbre CTL + explications

3.3 Syntaxe

Présentation détaillée de la syntaxe utilisée par CTL ainsi que ses différentes propriétés

3.4 Sémantique

Présentation de la sémantique de CTL - des relations de satisfactions, des interprétations des différentes formules, etc..

4 Le model-checking CTL : algorithme et implémentation

4.1 Pseudo-code de l'algorithme

Pseudo-code (ou code personnel) simple d'un algorithme de Model Checking CTL.

4.2 Analyse du code

Analyse détaillée du code de l'algorithme et exemple d'application

4.3 Complexité

Complexité du code donné ainsi que d'un model checking de CTL en général

FIN DU DOC : Sources, bibliographie

Bibliographie

[1] Baier, C. et Katoen, J.-P. (2008). *Principles of Model Checking*. The MIT Press. Cambridge, Massachusetts.

[2] Bourdil, P.-A. (2015). Contribution à la modélisation et la vérification formelle par model checking - symétries pour les réseaux de petri temporels. *Université de Toulouse*.

[3] Clarke, E. M. (2008). The birth of model checking. *Carnegie Mellon University, Department of Computer Science. Pittsburgh, PA, USA*.

[4] Edmund M. Clarke, William Klieber, M. N. P. Z. (2012). Model checking and the state explosion problem. *Carnegie Mellon University & ETH Zürich*.

[5] Finis, J. (2012). Incremental model checking of recursive kripke structures. *Augsburg University*.

[6] Freyja (2017). How much could software errors be costing your company ? `https://raygun.com/blog/cost-of-software-errors/`.

[7] Kripke, S. A. (1963). Semantical considerations on modal logic. *Acta philosophica fennica*, 16(1963) :83–94.

[8] Kuhtz, L. (2010). Model checking finite paths and trees. *Universität des Saarlandes, Saarbrücken*.

[9] Merz, S. (2010). An introduction to model checking.

[10] Schwoon, S. (2002). Model-checking pushdown systems. *Lehrstuhl für Informatik VII der Technischen Universität München*.