Automates et logique temporelle LTL

Souffan Nathan   Bouarah Romain
Supervisé par François Laroussinie

8 juin 2021

Le sujet

- Découvrir la logique LTL
- Reconnaître les modèles d'une formule LTL à l'aide d'un automate
- Implémenter la construction de cet automate

Utilité

Définition (Vérification de modèles)

La vérification de modèles, ou *model checking*, consiste à vérifier certaines propriétés sur le modèle d'un système.

Utilité

Définition (Vérification de modèles)

La vérification de modèles, ou *model checking*, consiste à vérifier certaines propriétés sur le modèle d'un système.

Exemple

- On souhaite vérifier la *sûreté et réactivité* d'un *ascenceur*

Utilité

Définition (Vérification de modèles)

La vérification de modèles, ou *model checking*, consiste à vérifier certaines propriétés sur le modèle d'un système.

Exemple

- On souhaite vérifier la *sûreté et réactivité* d'un *ascenceur*
- Vérifier qu'il n'y a *pas d'interblocage* dans un *programme concurrentiel*

Les logiques temporelles

Les logiques temporelles

Plusieurs logiques temporelles :

- *Computation tree logic* (CTL) ou logique du temps arborescent

Les logiques temporelles

Plusieurs logiques temporelles :

- *Computation tree logic* (CTL) ou logique du temps arborescent
- *linear temporal logic* (LTL) ou Logique temporelle de temps linéaire

Les logiques temporelles

Plusieurs logiques temporelles :

- *Computation tree logic* (CTL) ou logique du temps arborescent
- *linear temporal logic* (LTL) ou Logique temporelle de temps linéaire
- *Signal Temporal Logic*, *Metric Interval Temporal Logic*, ...

Syntaxe

Soient f_1, f_2 des formules LTL et $p \in AP$ une proposition atomique.
Une formule LTL f peut s'écrire comme :

- p : atome
- $\top$: tautologie
- $\neg f_1$: négation
- $f_1 \wedge f_2$: conjonction

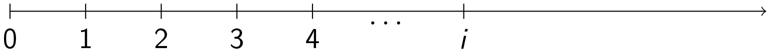
Syntaxe

Soient f_1, f_2 des formules LTL et $p \in AP$ une proposition atomique.
Une formule LTL f peut s'écrire comme :

- p : atome
- $\top$: tautologie
- $\neg f_1$: négation
- $f_1 \wedge f_2$: conjonction
- Xf_1 : suivant
- $f_1 U f_2$: jusqu'à

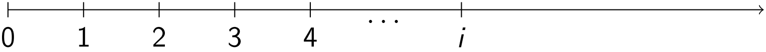
Sémantique

On interprète une formule sur une position $i \geq 0$ le long d'une exécution étiquetée (p, l) où $p \in Q^\omega$ et $l : Q \to 2^{AP}$



Sémantique

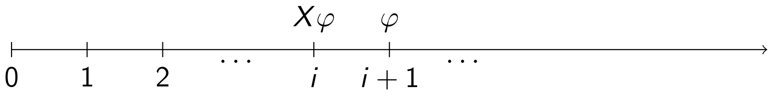
On interprète une formule sur une position $i \geq 0$ le long d'une exécution étiquetée (p, l) où $p \in Q^\omega$ et $l : Q \to 2^{AP}$



- $p, l, i \models v \Leftrightarrow v \in l(p(i))$ où $v \in AP$
- $p, l, i \models \top$
- $p, l, i \models \neg\varphi \Leftrightarrow p, l, i \not\models \varphi$
- $p, l, i \models \varphi \wedge \psi \Leftrightarrow [(p, l, i \models \varphi) \wedge (p, l, i \models \psi)]$

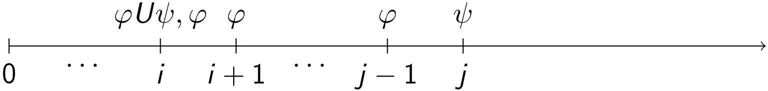
Sémantique de *suivant*

$$p, l, i \models X\varphi \Leftrightarrow p, l, i+1 \models \varphi$$



Sémantique de *jusqu'à*

$$p, l, i \models \varphi U \psi \Leftrightarrow$$
$$[\exists j \geq i \quad (p, l, j \models \psi) \wedge (\forall i \leq k < j \quad p, l, k \models \varphi)]$$



Quelques exemples

$a, b \in AP$

- GFa : (toujours(futur a)) ce qui signifie il y a une infinité de positions où a est vrai.

Quelques exemples

$a, b \in AP$

- GFa : (toujours(futur a)) ce qui signifie il y a une infinité de positions où a est vrai.
- $aU(Gb)$: a est vrai tant que b est faux, dès que a est faux, b est toujours vrai par la suite

Définition (Automate de Büchi)

Un automate de Büchi est un quintuplet $\mathcal{A} = (\Sigma, Q, Q_I, \Delta, \mathscr{F})$ où :

- Σ est un alphabet
- Q est l'ensemble des états
- $Q_I \subseteq Q$ est l'ensemble des états initiaux.
- $\Delta \subseteq Q \times \Sigma \times Q$ est l'ensemble des transitions.
- $\mathscr{F} \subseteq Q$ est l'ensemble des états finaux. Un mot w est accepté s'il existe une exécution acceptante de $\mathcal{A}$ sur w.

Un exemple d'automate de Büchi

Soit $\mathcal{A} = (\{a, b\}, \{q_0, q_1\}, \{q_0\}, \Delta, \{q_1\})$ un automate de Büchi.
L'ensemble des transitions Δ est donné dans la figure.

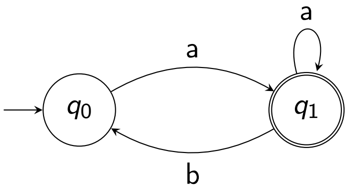


Figure – Représentation graphique de $\mathcal{A}$

Définition (Exécution)

Soit $w \in \Sigma^\omega$ un mot infini. Une exécution de $\mathcal{A}$ sur w est une suite infinie $\rho = q_0 q_1 q_2 \cdots \in Q^\omega$ telle que :

$$\forall i \geq 0 \quad (q_i, w_i, q_{i+1}) \in \Delta$$

Définition (Exécution)

Soit $w \in \Sigma^\omega$ un mot infini. Une exécution de $\mathcal{A}$ sur w est une suite infinie $\rho = q_0 q_1 q_2 \cdots \in Q^\omega$ telle que :

$$\forall i \geq 0 \quad (q_i, w_i, q_{i+1}) \in \Delta$$

Définition (Exécution acceptante)

$\rho \in Q^\omega$ une exécution de $\mathcal{A}$ est dite acceptante si :

$$Etats_{\#\infty}(\rho) \cap \mathscr{F} \neq \varnothing$$

où $Etats_{\#\infty}(\rho)$ est l'ensemble des états apparaissants une infinité de fois dans ρ.

Un exemple d'automate de Büchi

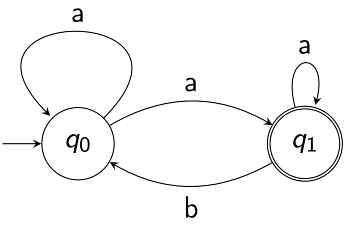


Figure – Un automate de Büchi

Pour le mot a^ω, on a :

- $q_0 q_0 \dots$ qui est une exécution

Un exemple d'automate de Büchi

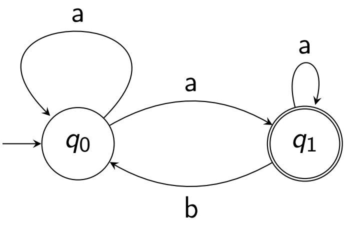


Figure – Un automate de Büchi

Pour le mot a^ω, on a :

- $q_0 q_0 \ldots$ qui est une exécution
- $q_0 q_1 \ldots$ qui est une exécution acceptante

Un exemple d'automate de Büchi

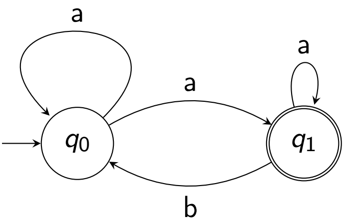


Figure – Un automate de Büchi

Pour le mot a^ω, on a :

- $q_0 q_0 \ldots$ qui est une exécution
- $q_0 q_1 \ldots$ qui est une exécution acceptante
- ...

Automate de Büchi généralisé

Définition (Automate de Büchi généralisé)

Un automate de Büchi généralisé est un quintuplet $\mathcal{A} = (\Sigma, Q, Q_I, \Delta, \mathscr{F})$ où :

- Σ, Q, Q_I, Δ sont comme précédemment.
- $\mathscr{F} \subseteq \mathcal{P}(Q)$ est la condition d'acceptation. $\mathscr{F}$ est un ensemble d'ensembles finaux. De même, un mot w est accepté s'il existe une exécution acceptante de $\mathcal{A}$ sur w.

$\forall G \in \mathscr{F}$ on passe infiniment de fois par l'un des états de G.

Sous formules

Définition

On note $SubF(\varphi)$ l'ensemble des sous formules de φ et leur négation.

Sous formules

Définition

On note $SubF(\varphi)$ l'ensemble des sous formules de φ et leur négation.

Exemple

Si $\varphi = aUb$ alors $SubF(\varphi) = \{a, \neg a, b, \neg b, aUb, \neg(aUb)\}$.

Définition (Sous-ensemble cohérent)

$q \in 2^{SubF(\varphi)}$ est cohérent si :

(i) $\bot \notin q$.

(ii) Si $\psi_1 \wedge \psi_2 \in q$ alors $\psi_1 \in q$ et $\psi_2 \in q$.

(iii) Si $\psi_1 \vee \psi_2 \in q$ alors $\psi_1 \in q$ ou $\psi_2 \in q$.

(iv) $\psi \in q \iff \neg\psi \notin q$.

Définition (Sous-ensemble cohérent)

$q \in 2^{SubF(\varphi)}$ est cohérent si :

(i) $\perp \notin q$.
(ii) Si $\psi_1 \wedge \psi_2 \in q$ alors $\psi_1 \in q$ et $\psi_2 \in q$.
(iii) Si $\psi_1 \vee \psi_2 \in q$ alors $\psi_1 \in q$ ou $\psi_2 \in q$.
(iv) $\psi \in q \iff \neg\psi \notin q$.

Définition (Sous-ensemble maximal)

$q \in 2^{SubF(\varphi)}$ est maximal si pour tout $\psi \in SubF(\varphi)$ on a soit $\psi \in q$ soit $\neg\psi \in q$.

Définition (Sous-ensemble cohérent)

$q \in 2^{SubF(\varphi)}$ est cohérent si :

(i) $\perp \notin q$.
(ii) Si $\psi_1 \wedge \psi_2 \in q$ alors $\psi_1 \in q$ et $\psi_2 \in q$.
(iii) Si $\psi_1 \vee \psi_2 \in q$ alors $\psi_1 \in q$ ou $\psi_2 \in q$.
(iv) $\psi \in q \iff \neg\psi \notin q$.

Définition (Sous-ensemble maximal)

$q \in 2^{SubF(\varphi)}$ est maximal si pour tout $\psi \in SubF(\varphi)$ on a soit $\psi \in q$ soit $\neg\psi \in q$.

Définition (Sous-ensemble conforme à la sémantique de LTL)

$q \in 2^{SubF(\varphi)}$ est conforme à la sémantique de LTL :

(i) Si $\psi_1 U \psi_2 \in q$ alors on a soit $\psi_1 \in q$ soit $\psi_2 \in q$.
(ii) $\forall \psi_1 U \psi_2 \in SubF(\varphi)$ si $\psi_2 \in q$ alors $\psi_1 U \psi_2 \in q$.

Un exemple

Soit $\varphi = aU(Xb)$ alors

$$SubF(\varphi) = \{a, \neg a, b, \neg b, Xb, \neg(Xb), aU(Xb), \neg(aU(Xb))\}$$

Un exemple

Soit $\varphi = aU(Xb)$ alors

$$SubF(\varphi) = \{a, \neg a, b, \neg b, Xb, \neg(Xb), aU(Xb), \neg(aU(Xb))\}$$

1. $q_1 = \{\neg a, b, Xb, aU(Xb)\}$ est un sous-ensemble cohérent, maximal et conforme à la sémantique de LTL.

Un exemple

Soit $\varphi = aU(Xb)$ alors

$$SubF(\varphi) = \{a, \neg a, b, \neg b, Xb, \neg(Xb), aU(Xb), \neg(aU(Xb))\}$$

1. $q_1 = \{\neg a, b, Xb, aU(Xb)\}$ est un sous-ensemble cohérent, maximal et conforme à la sémantique de LTL.
2. $q_2 = \{\neg a, b, Xb, \neg(aU(Xb))\}$ est un sous-ensemble cohérent, maximal mais non conforme à la sémantique de LTL car on a Xb et $\neg(aU(Xb))$.

On pose $\mathcal{A}_\varphi = (2^{AP}, Q, Q_I, \Delta, \mathscr{F})$ où :

- $Q \subseteq 2^{SubF(\varphi)}$ contient tout les sous-ensembles cohérents, maximaux et conformes à la sémantique de LTL.
- $Q_I = \{q \in Q | \varphi \in q\}$
- $(q, a, q') \in \Delta$ si :
  - (i) $\forall p \in AP \quad p \in q \iff p \in a$ (i.e. a possède toutes les propositions atomiques de q)
  - (ii) $\forall X\psi \in SubF(\varphi) \quad X\psi \in q \iff \psi \in q'$
  - (iii) $\forall \psi_1 U \psi_2 \in SubF(\varphi) \quad \psi_1 U \psi_2 \in q \iff (\psi_2 \in q \vee (\psi_1 \in q \wedge \psi_1 U \psi_2 \in q'))$
- $\mathscr{F} = \{F_{\psi_1 U \psi_2} | \psi_1 U \psi_2 \in SubF(\varphi)\}$ où

$$F_{\psi_1 U \psi_2} = \{q \in Q | \psi_1 U \psi_2 \notin q \vee \psi_2 \in q\}$$

Exemple pour $\varphi = Xa$

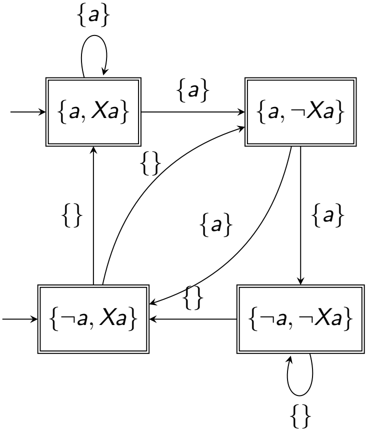


Figure – l'automate de Büchi généralisé pour Xa sur $\{a\}$

Correction de la construction

Théorème

Soit φ une formule LTL sur AP. On a, $\mathcal{L}(\mathcal{A}_\varphi) = mod(\varphi)$ où $mod(\varphi)$ est l'ensemble des modèles reconnues par φ.

Lemme

Soit $\omega \in (2^{AP})^\omega$ *et* $p = q_0 q_1 \ldots$ *une exécution acceptante de* $\mathcal{A}_\varphi$ *du mot* ω *alors :*

$\forall i \geq 0, \forall \psi \in SubF(\varphi) : \ (\psi \in q_i \Leftrightarrow \omega_i \models \varphi)$

Démonstration.

Par induction structurelle sur ψ

Démonstration.

Par induction structurelle sur ψ

- $\psi = v \in AP$

Démonstration.

Par induction structurelle sur ψ

- $\psi = v \in AP$
- $\psi = \psi_1 \wedge \psi_2$

Démonstration.

Par induction structurelle sur ψ

- $\psi = v \in AP$
- $\psi = \psi_1 \wedge \psi_2$
- $\psi = \neg\psi_1$

Démonstration.

Par induction structurelle sur ψ

- $\psi = v \in AP$
- $\psi = \psi_1 \wedge \psi_2$
- $\psi = \neg\psi_1$
- $\psi = X\psi_1$

Démonstration.

Par induction structurelle sur ψ

- $\psi = v \in AP$
- $\psi = \psi_1 \wedge \psi_2$
- $\psi = \neg\psi_1$
- $\psi = X\psi_1$
- $\psi = \psi_1 U \psi_2$

$\square$

$\mathcal{L}(\mathcal{A}_\varphi) \supseteq mod(\varphi)$

Lemma

Si $w \in (2^{AP})^\omega$ *un mot infini sur l'alphabet* 2^{AP} *tel que* $w, 0 \models \varphi$ *alors* $w \in \mathcal{L}(\mathcal{A}_\varphi)$.

$\mathcal{L}(\mathcal{A}_\varphi) \supseteq mod(\varphi)$

Lemma

Si $w \in (2^{AP})^\omega$ un mot infini sur l'alphabet 2^{AP} tel que $w, 0 \models \varphi$ alors $w \in \mathcal{L}(\mathcal{A}_\varphi)$.

Démonstration.

1. $\forall i \geq 0 \quad q_i = \{\psi \in SubF(\varphi) | w, i \models \psi\}$ et $\rho = q_0 q_1 q_2 \ldots$

$\square$

$\mathcal{L}(\mathcal{A}_\varphi) \supseteq mod(\varphi)$

Lemma

Si $w \in (2^{AP})^\omega$ un mot infini sur l'alphabet 2^{AP} tel que $w, 0 \models \varphi$ alors $w \in \mathcal{L}(\mathcal{A}_\varphi)$.

Démonstration.

1. $\forall i \geq 0 \quad q_i = \{\psi \in SubF(\varphi) | w, i \models \psi\}$ et $\rho = q_0 q_1 q_2 \ldots$
2. $w, 0 \models \varphi$ donc $\varphi \in q_0$ donc q_0 est bien un état initial.

$\square$

$\mathcal{L}(\mathcal{A}_\varphi) \supseteq mod(\varphi)$

Lemma

Si $w \in (2^{AP})^\omega$ un mot infini sur l'alphabet 2^{AP} tel que $w, 0 \models \varphi$ alors $w \in \mathcal{L}(\mathcal{A}_\varphi)$.

Démonstration.

1. $\forall i \geq 0 \quad q_i = \{\psi \in SubF(\varphi) | w, i \models \psi\}$ et $\rho = q_0 q_1 q_2 \dots$
2. $w, 0 \models \varphi$ donc $\varphi \in q_0$ donc q_0 est bien un état initial.
3. Il y a bien des transition (q_i, w_i, q_{i+1}) dans $\mathcal{A}_\varphi$.

$\square$

$\mathcal{L}(\mathcal{A}_\varphi) \supseteq mod(\varphi)$

Lemma

Si $w \in (2^{AP})^\omega$ un mot infini sur l'alphabet 2^{AP} tel que $w, 0 \models \varphi$ alors $w \in \mathcal{L}(\mathcal{A}_\varphi)$.

Démonstration.

1. $\forall i \geq 0 \quad q_i = \{\psi \in SubF(\varphi) | w, i \models \psi\}$ et $\rho = q_0 q_1 q_2 \dots$
2. $w, 0 \models \varphi$ donc $\varphi \in q_0$ donc q_0 est bien un état initial.
3. Il y a bien des transition (q_i, w_i, q_{i+1}) dans $\mathcal{A}_\varphi$.
4. si $\psi_1 U \psi_2 \in q_i$, alors $w, i \models \psi_1 U \psi_2$ (par construction des q_i) donc $\exists j \geq i$ tel que $w, j \models \psi_2$ et $\forall k, i \leq k < j \quad w, k \models \psi_1$. Enfin, on a aussi $\psi_1 U \psi_2 \in q_j$ et il existe un chemin valide jusqu'à q_j ainsi ρ passe infiniment souvent par $F_{\psi_1 U \psi_2}$.

$\square$