TD2 de Model Checking

Logiques temporelles

Exercice 1. *Questions très simples sur les connecteurs temporels (regardez la définition formelle) :*
- $\mathbf{F}p$ *est-il vrai si* p *vrai tout de suite dans l'état courant ?*
- $\mathbf{G}p$ *est-il vrai si* p *faux dans l'état courant et vrai partout ailleurs ?*
- $p\mathbf{U}q$ *est-il vrai si* p *faux et* q *vrai dans l'état courant ?*
- $p\mathbf{U}q$ *est-il vrai si* q *est toujours faux, et* p *toujours vrai ?*

Exercice 2. *Dessinez des dépliages sur lesquels vous illustrerez les propriétés* **EX**, **AX**, **EU**, **AU**.

Exercice 3. *Exprimer les propriétés suivantes :*

1. *Tous les états satisfont* p.
2. *On peut atteindre* p *par un chemin où* q *est toujours vrai.*
3. *Quelquesoit l'état, on finit par aller à un état où* p *vrai.*
4. *Quelquesoit l'état, on peut aller à un état où* p *vrai.*
5. *Absence de deadlock.*

Exercice 4. *On va voir que certains connecteurs sont redondants.*
- *Exprimer* $\mathbf{G}p$ *avec les connecteurs* $\neg, \mathbf{F}$ *et* p. *(prouvez le)*
- *Exprimer* $\mathbf{F}p$ *grâce au connecteur* $\mathbf{U}$. *(prouvez le)*
- *Peut-on exprimer* $\mathbf{X}$ *en fonction des autres connecteurs ? (prouvez le)*
- *Peut-on exprimer* $\mathbf{U}$ *en fonction des autres connecteurs ? (une réponse intuitive suffit)*

Exercice 5 (Autres connecteurs.)**.** *On va définir quelques connecteurs additionels utiles.*

1. *Définir formellement la relation* $\models$ *pour les connecteurs suivants :*

- $p\mathbf{W}q$ *(weak until) : signifie que* p *est vrai jusqu'à ce que* q *soit vrai, mais* q *n'est pas forcément vrai à un moment. Dans ce cas,* p *reste vrai tout le long du chemin.*
- $\mathbf{F}^{\infty}p$ *(infiniment souvent) :* p *est infiniment vrai au long de l'exécution.*
- $\mathbf{G}^{\infty}p$ *(presque toujours) : à partir d'un moment donné,* p *est toujours vrai.*
- $p\ \mathbf{U}_{\leq \mathbf{k}}q$ *(bounded until) :* p *vrai jusqu'à ce que* q *soit vrai, et* q *avant au plus* k *observations.*
- $p\mathbf{R}q$ *(release) :* q *est vraie jusqu'à (et inclus) le premier état où* p *est vraie, et* p *n'est pas forcément vraie un jour.*

2. *On va maintenant faire le lien entre ces connecteurs et les anciens.*

- *Exprimer* $\mathbf{F}^{\infty}$, $\mathbf{G}^{\infty}$, $\mathbf{W}$, $\mathbf{U}_{\leq \mathbf{k}}$, $\mathbf{R}$ *par des connecteurs basiques de LTL (pour* $\mathbf{U}_{\leq \mathbf{k}}$ *: juste avec* $\mathbf{X}$*).*
- *Exprimer* $\mathbf{U}$ *uniquement avec* $\mathbf{W}$ *(ni* $\mathbf{U}$*, ni* $\mathbf{G}$ *ni* $\mathbf{F}$*).*

Exercice 6 (CTL*)**.**

1. *Montrer que* $\vee$, $\neg$, $\mathbf{X}$, $\mathbf{U}$ *et* $\mathbf{E}$ *suffisent à exprimer les autres connecteurs.*

2. *Montrez que si on ajoute* $\mathbf{R}$*, on peut restreindre* $\neg$ *aux propositions atomiques.*

Exercice 7 (CTL)**.** *Montrer que* p*,* $\vee$*,* $\neg$*,* $\mathbf{EX}$*,* $\mathbf{EG}$ *et* $\mathbf{EU}$ *suffisent à exprimer les autres connecteurs. Montrer ensuite que* p*,* $\wedge$*,* $\neg$*,* $\mathbf{EX}$*,* $\mathbf{AU}$ *et* $\mathbf{EU}$ *suffisent aussi.*

Exercice 8. *Ce n'est pas parcequ'une formule n'est pas syntaxiquement dans CTL qu'il n'y a pas de formule CTL équivalente. Tranformez les formules suivantes en formules CTL :* $\mathbf{E}(p \wedge \mathbf{F}q)$*,* $\mathbf{AF}^{\infty}p$*,* $\mathbf{EG}^{\infty}p$*.*

Montrer qu'on peut exprimer les formules suivantes en CTL : $\mathbf{AW}$*,* $\mathbf{EW}$*,* $\mathbf{AU}_{\leq \mathbf{k}}$*,* $\mathbf{EU}_{\leq \mathbf{k}}$ *?*

Par contre on ne peut pas exprimer $\mathbf{EF}^{\infty}$ *ni* $\mathbf{AG}^{\infty}$*. Montrez que* $\mathbf{EGF}p \neq \mathbf{EGEF}p$*. Montrez que* $\mathbf{AFG}p \neq \mathbf{AFAG}p$*.*

Exercice 9 (Théorème de Kamp (*))**.** *Ce résultat est le sens (facile) du théorème de Kamp, qui établit que LTL a même pouvoir d'expression que la logique monadique du premier ordre à un successeur.*

On se donne un ensemble AP de prédicats atomiques $P : \mathbb{N} \to \mathcal{B}$ *et un ensemble Var de variables. On considère la logique monadique du premier ordre à un successeur, définie par :*

. $t := 0 | v \in Var | t + 1$

. $atome := t \geq t | t = t | P(t), P \in AP$

. $f := f \vee f | f \wedge f | \neg f | \exists v, f | atome$

La logique est interprétée sur $\mathbb{N}$*. En considérant que* $P(t)$ *signifie que la propriété* P *est vrai au temps* t *(=* P *vrai à la* t*-ième étape du chemin), donner une traduction (récursive) des formules LTL* φ *en formules* $\widetilde{\varphi}$ *de logique monadique ayant même signification.*

Exercice 10 (Équivalence comportementale (*).)**.** *Soit deux structures de Kripke* $\mathcal{M}_1$ *et* $\mathcal{M}_2$ *et* φ *une propriété LTL. On suppose que* $\mathcal{M}_1 \models \varphi$*. Que peut-on dire si :*

1. $\mathcal{L}(\mathcal{M}_1) = \mathcal{L}(\mathcal{M}_2)$ *?*
2. $\mathcal{L}(\mathcal{M}_2) \subseteq \mathcal{L}(\mathcal{M}_1)$ *?*
3. $\mathcal{L}(\mathcal{M}_1) \subseteq \mathcal{L}(\mathcal{M}_2)$ *?*

On suppose maintenant que φ *est une propriété CTL. Reprendre la question 1.*

Exercice 11 (**)**.** *Montrer que le problème du model checking de LTL se ramène au problème de la validité de LTL. Plus précisément, on se donne une formule LTL* φ *et une structure de Kripke* $\mathcal{M} = \langle Q, \to, P, l, s_0 \rangle$*. On va construire une formule* φ'' *telle que* $\mathcal{M}, s_0 \models \varphi$ *ssi* φ'' *est valide. Pour cela on va construire une formule* φ' *telle que* $\sigma \models \varphi'$ *ssi* $\sigma \in \mathcal{L}(\mathcal{M})$*. On commence par rajouter une variable propositionnelle* p_{s_i} *pour chaque état* s_i *de* $\mathcal{M}$*.*

1. *Construisez les formules suivantes :* $PROP_{s_i}$ *qui indique les propriétés atomiques vérifiées par* s_i *et* $NEXT_{s_i}$ *qui mime la relation de transition de* $\mathcal{M}$*.*
2. *Servez-vous des résultats précédents pour construire* φ'*.*
3. *Concluez en construisant la formule* φ'' *cherchée à partir de* φ' *et* φ*.*