Correction TD de Model Checking

Logiques temporelles

Exercice 1. *La vivacité est-elle de la sûreté ? Justifiez.*

Correction. La vivacité est différente de la sûreté car pour une exécution qui ne satisfait pas par exemple $\mathbf{F}p$, on ne peut déduire qu'elle est fausse en regardant juste un préfixe passé. □

Exercice 2. *Quelques petits exercices sur les connecteurs temporels :*
- $\mathbf{F}p$ *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 ?*

Correction. oui, non, oui, non □

Exercice 3. *Dessinez des dépliages sur lesquels vous illustrerez les propriétés* $\mathbf{EX}$, $\mathbf{AX}$, $\mathbf{EU}$, $\mathbf{AU}$.

Correction. Attention pour $\mathbf{E}p\mathbf{U}q$ et $\mathbf{A}p\mathbf{U}q$ à ce que p soit vrai au début (si q faux). □

Exercice 4. *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 revenir à l'état initial init.*
4. *Quelquesoit l'état, on peut revenir à l'état initial init.*
5. *Absence de deadlock (partiel).*

Correction.

1. $\mathbf{AG}p$ (classique de l'invariance)
2. $\mathbf{E}(\mathbf{F}p \wedge \mathbf{G}q)$, ou bien $\mathbf{E}(q\mathbf{U}p)$ selon le sens que l'on donne à la phrase (voyez-vous la différence ?)
3. $\mathbf{AGAF}p$ (d'autres traductions comme $\mathbf{AF}p$ se basent sur le fait que "init" est initial, mais seraient fausses pour d'autres propriétés. Désolé l'exemple n'est pas très bon)
4. $\mathbf{AGEF}p$
5. $\mathbf{AGEX}true$ (vu la sémantique, ne peut être faux que si il existe un état sans successeur ; c'est plus une astuce à avoir vue que quelquechose de vraiment utile).

□

Exercice 5. *On va voir que certains connecteurs sont redondants.*

1. *Exprimer* $\mathbf{G}p$ *avec les connecteurs* $\neg, \mathbf{F}$ *et* p.
2. *Exprimer* $\mathbf{F}p$ *grâce au connecteur* $\mathbf{U}$.
3. *Peut-on exprimer* $\mathbf{X}$ *en fonction des autres connecteurs ?*
4. *Peut-on exprimer* $\mathbf{U}$ *en fonction des autres connecteurs ?*

Correction.

1. $\mathbf{G}p \equiv \neg\mathbf{F}\neg p$
2. $\mathbf{F}p \equiv true\mathbf{U}p$
3. non. Difficile à démontrer, mais intuitivement $\mathbf{X}$ est le seul opérateur qui impose fortement quand doit avoir lieu l'observation (“au prochain coup, ni avant ni après”). Les autres connecteurs sont plus lâches.
4. non. Difficile à démontrer, mais intuitivement $\mathbf{U}$ est le seul opérateur qui combine deux sous-formules.

□

Exercice 6 (Autres connecteurs.)**.** *On va définir quelques connecteurs additionels utiles.*

1. *Définir la relation* $\models$ *pour les connecteurs additionnels 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 *vrai dans au plus* k *observations.*
- $p\mathbf{R}q$ *(release) :* q *est vraie jusqu'à (et inclus) le premier état où* p *est vraie, sachant que* p *n'est pas forcément vraie un jour.*

2. *On va maintenant faire le lien entre ces connecteurs et les anciens.*
- *Exprimer* $\mathbf{F}^\infty$, $\mathbf{G}^\infty$, $\mathbf{W}$, $\mathbf{U}_{\leq \mathbf{k}}$ *par des connecteurs de basiques de LTL.*
- *Exprimer* $\mathbf{U}$ *dans LTL-*$\mathbf{U}$*+*$\mathbf{W}$.

Correction.

1.
- $\sigma \models \varphi_1\mathbf{W}\varphi_2$ iff (il existe $k \geq 0$ tel que $\sigma^k \models \varphi_2$ et pour tout $0 \leq j < k$ $\sigma^j \models \varphi_1$) ou pour tout k $\sigma^k \models \varphi_1$
- $\sigma \models \mathbf{F}^\infty\varphi$ iff pour tout k, il existe $j \geq k$ tel que $\sigma^j \models \varphi$
- $\sigma \models \mathbf{G}^\infty\varphi$ iff il existe k tel que pour tout $j \geq k$ on a $\sigma^j \models \varphi$
- $\sigma \models \varphi_1\mathbf{U}_{\leq \mathbf{k}}\varphi_2$ iff il existe $0 \leq i \leq k$ tel que $\sigma^i \models \varphi_2$ et pour tout $0 \leq j < i$ $\sigma^j \models \varphi_1$

2.
- $p\mathbf{W}q \equiv (p\mathbf{U}q) \vee \mathbf{G}p$; $\mathbf{F}^\infty p \equiv \mathbf{GF}p$; $\mathbf{G}^\infty p \equiv \mathbf{FG}p$;
  Deux traductions pour $\mathbf{U}_{\leq \mathbf{k}}$:
  $p\mathbf{U}_{\leq \mathbf{k}}q \equiv p\mathbf{U}q \wedge (q \vee \mathbf{X}q \vee \ldots \vee \mathbf{X}^k q)$
  ou
  $p\mathbf{U}_{\leq \mathbf{k}}q \equiv (q \vee (p \wedge \mathbf{X}q) \vee \ldots \vee (p \wedge \mathbf{X}p \wedge \ldots \wedge \mathbf{X}^{k-1}p \wedge \mathbf{X}^k q))$
- $p\mathbf{U}q \equiv (p\mathbf{W}q) \wedge \mathbf{F}q$, et $\mathbf{F}$ s'obtient à partir de $\mathbf{G}$, car $\mathbf{G}p \equiv p\mathbf{W}false$

□

Exercice 7. *Parmi les opérateurs suivants, lesquels correspondent plutôt à des propriétés de sûreté ?* $\mathbf{X}, \mathbf{F}, \mathbf{G}, \mathbf{U}, \mathbf{W}, \mathbf{U}_{\leq \mathbf{k}}, \mathbf{F}^\infty, \mathbf{G}^\infty$.

Correction. Réfléchir en termes de contre-exemple finis ou non. Sûreté (ou sous-classes de sûreté) : $\mathbf{X}, \mathbf{G}, \mathbf{W}, \mathbf{U}_{\leq \mathbf{k}}$

□

Exercice 8. *Exprimer en langage naturel les propriétés suivantes.*

- $\mathbf{AG}(emission \rightarrow \mathbf{F}reception)$

– $\mathbf{AF}^\infty ok \rightarrow \mathbf{G}(emission \rightarrow \mathbf{F}reception)$

Correction. 1. Pour tout chemin, une émission (de message) est toujours suivi par une réception (de message)

2. pour tout chemin, si on a infiniment souvent "ok", alors une émission (de message) est toujours suivi par une réception (de message).

□

Exercice 9. *Exprimer toutes les propriétés de la section 3.1 en tenant compte des quantificateurs de chemin.*

Correction.

□

Exercice 10 (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.*

Correction.

1. On revient à l'exo 11 pour exprimer $\mathbf{F}$ et $\mathbf{G}$, bien entendu $\varphi_1 \wedge \varphi_2 \equiv \neg(\neg\varphi_1 \vee \neg\varphi_2)$, et on vérifie que $\mathbf{A}\varphi \equiv \neg\mathbf{E}\neg\varphi$

□

Exercice 11 (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.*

Correction. Le second est plus facile.

1. On traduit les opérateurs manquants comme suit :
$\mathbf{AX}\varphi \equiv \neg\mathbf{EX}\neg\varphi$
$\mathbf{AF}\varphi \equiv \neg\mathbf{EG}\neg\varphi$
$\mathbf{EF}\varphi \equiv \mathbf{E}true\mathbf{U}\varphi$
$\mathbf{AG}\varphi \equiv \neg\mathbf{EF}\neg\varphi$
$\mathbf{A}\varphi_1\mathbf{U}\varphi_2 \equiv \neg((\mathbf{E}(\varphi_1 \wedge \neg\varphi_2)\mathbf{U}(\neg\varphi_1 \wedge \neg\varphi_2)) \vee (\mathbf{EG}\neg\varphi_2))$

2. On traduit les opérateurs manquants comme suit :
$\mathbf{AX}\varphi \equiv \neg\mathbf{EX}\neg\varphi$
$\mathbf{AF}\varphi \equiv \mathbf{A}true\mathbf{U}\varphi$
$\mathbf{EF}\varphi \equiv \mathbf{E}true\mathbf{U}\varphi$
$\mathbf{AG}\varphi \equiv \neg\mathbf{EF}\neg\varphi$
$\mathbf{EG}\varphi \equiv \neg\mathbf{AF}\neg\varphi$

□