

IGL502/752 – Techniques de vérification et de validation
Université de Sherbrooke

Devoir 1

Enseignant:	Michael Blondin
Date de remise:	mardi 22 septembre 2020 à 23h59
À réaliser:	à deux ou individuellement au 1 ^{er} cycle individuellement aux cycles supérieurs
Modalités:	remettre en ligne sur Turnin
Bonus:	les questions bonus sont indiquées par ★
Pointage:	sur 30 points au 1 ^{er} cycle sur 38 points aux cycles supérieurs

Question 1.

Considérons le système concurrent \mathcal{S} suivant constitué de deux processus qui partagent deux variables booléennes $b_0, b_1 \in \{\text{faux}, \text{vrai}\}$ et une variable binaire $k \in \{0, 1\}$:

```

 $b_0 \leftarrow \text{faux}$ 
 $b_1 \leftarrow \text{faux}$ 
 $k \leftarrow 0$ 
lancer processus(0) et processus(1) de façon concurrente

```

```

processus( $i$ ) :
  boucler
1    $b_i \leftarrow \text{vrai}$ 
2   tant que  $k \neq i$  faire
3     tant que  $b_{1-i}$  faire rien
4      $k \leftarrow i$ 
5     /* section critique */
6      $b_i \leftarrow \text{faux}$ 

```

(a) En vous inspirant des exemples du cours, expliquez brièvement comment modéliser \mathcal{S} à l'aide d'un système de transition $\mathcal{T} = (S, \rightarrow, I)$. Plus précisément, décrivez l'ensemble des états S et des états initiaux I , et expliquez le sens que vous donnez à un état de S . 3 pts

(b) Donnez une représentation graphique partielle de \mathcal{T} . Plus précisément, dessinez les états $I \cup \text{Post}(I) \cup \text{Post}(\text{Post}(I))$ et les transitions entre ces états. 2 pts

★ Donnez un chemin fini de \mathcal{T} qui atteint un état où processus(0) et processus(1) sont tous deux dans leur section critique. ★ 1 pt

Question 2.

9 pts

Soient $AP = \{p, q, r\}$ et les formules LTL suivantes sur AP :

$$\varphi_1 = FG(p \vee r), \quad \varphi_2 = G(p \cup (\text{X}q)), \quad \varphi_3 = G[(\text{X}\neg r) \rightarrow (F(p \wedge q))].$$

Pour chacun des mots infinis σ_i suivants, dites quelles formules parmi φ_1 , φ_2 et φ_3 sont satisfaites par σ_i . Justifiez vos réponses.

- (a) $\sigma_1 = \{p\}\{p\}\{p, q\}\{r\}^\omega$, (b) $\sigma_2 = \emptyset(\{p\}\{q, r\})^\omega$, (c) $\sigma_3 = (\{p, q\}\emptyset)^\omega$.

Question 3.

8 pts

Soit $AP = \{e, r, a\}$ un ensemble de propositions atomiques satisfaites lorsqu'un processus: **e**nvoie un message, **r**eçoit un message, et **a**nnonce un résultat, respectivement.

- Spécifiez les propriétés suivantes en formules LTL sur AP ;
- Pour chacune de vos formules, donnez un mot infini (de votre choix) qui satisfait la formule et un mot infini (de votre choix) qui ne satisfait pas la formule.

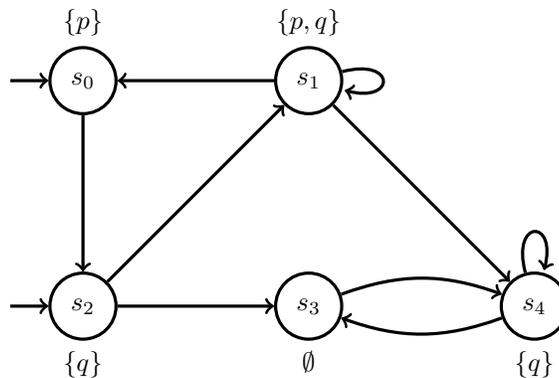
- (a) Le processus annonce au moins un résultat;
 (b) Le processus annonce au plus un résultat;
 (c) Le processus n'envoie et ne reçoit plus de messages après l'annonce d'un résultat;
 (d) Chaque fois que le processus envoie un message, il renvoie un message tant qu'il ne reçoit pas de réponse.

Si vous jugez que la propriété écrite en français est ambiguë, expliquez l'interprétation que vous en faites.

Question 4.

8 pts

Soit $\mathcal{T} = (S, \rightarrow, I, AP, L)$ la structure de Kripke telle que $S = \{s_0, s_1, s_2, s_3, s_4\}$, $I = \{s_0, s_2\}$, $AP = \{p, q\}$, et dont les transitions et la fonction d'étiquetage sont définies par:



- (a) Donnez le contenu des ensembles suivants: $\text{Pre}(s_0)$, $\text{Post}(s_3)$, $\text{Pre}^*(s_1)$, $\text{Post}^*(s_4)$;
 (b) Dites si \mathcal{T} satisfait la formule $\neg FG\neg q$. Justifiez votre réponse.
 (c) Dites si \mathcal{T} satisfait la formule $\text{XX}(\neg p \cup q)$. Justifiez votre réponse.
 (d) Dites si \mathcal{T} satisfait la formule $G(q \rightarrow F\neg p)$. Justifiez votre réponse.

Vous n'avez pas à répondre à cette question si vous êtes au premier cycle. Si vous y répondez, vous pourrez obtenir jusqu'à 2 points bonus.

☞ Question 5. (cycles supérieurs)

8 pts

LTL s'étend naturellement avec des opérateurs temporels qui raisonnent sur le passé. Par exemple, « $F^{-1}p$ » indique que la proposition atomique p est vraie au moment actuel ou à un moment du passé. Autrement dit, l'opérateur F^{-1} se comporte comme F , mais en remontant le temps vers zéro plutôt que l'infini. Cela peut être pratique pour spécifier des propriétés de façon plus succincte.

Cette extension requiert une légère redéfinition de la sémantique, puisque celle introduite dans les notes de cours « oublie le passé ». Plus formellement, on ajoute à la syntaxe les opérateurs X^{-1} , F^{-1} , G^{-1} et U^{-1} , et les formules sont interprétées sur une paire (σ, i) où $\sigma \in (2^{AP})^\omega$ est un mot infini et $i \in \mathbb{N}$ est une position de σ :

$$\begin{aligned}
 (\sigma, i) &\models \text{vrai} \\
 (\sigma, i) &\models p && \iff p \in \sigma(i) \\
 (\sigma, i) &\models \varphi_1 \wedge \varphi_2 && \iff (\sigma, i) \models \varphi_1 \wedge (\sigma, i) \models \varphi_2 \\
 (\sigma, i) &\models \varphi_1 \vee \varphi_2 && \iff (\sigma, i) \models \varphi_1 \vee (\sigma, i) \models \varphi_2 \\
 (\sigma, i) &\models \neg\varphi && \iff (\sigma, i) \not\models \varphi \\
 \\
 (\sigma, i) &\models X\varphi && \iff (\sigma, i+1) \models \varphi \\
 (\sigma, i) &\models F\varphi && \iff \exists j \geq i : (\sigma, j) \models \varphi \\
 (\sigma, i) &\models G\varphi && \iff \forall j \geq i : (\sigma, j) \models \varphi \\
 (\sigma, i) &\models \varphi_1 U \varphi_2 && \iff \exists j \geq i : ((\sigma, j) \models \varphi_2) \wedge (\forall i \leq \ell < j : (\sigma, \ell) \models \varphi_1) \\
 \\
 (\sigma, i) &\models X^{-1}\varphi && \iff i > 0 \wedge (\sigma, i-1) \models \varphi \\
 (\sigma, i) &\models F^{-1}\varphi && \iff \exists 0 \leq j \leq i : (\sigma, j) \models \varphi \\
 (\sigma, i) &\models G^{-1}\varphi && \iff \forall 0 \leq j \leq i : (\sigma, j) \models \varphi \\
 (\sigma, i) &\models \varphi_1 U^{-1} \varphi_2 && \iff \exists 0 \leq j \leq i : ((\sigma, j) \models \varphi_2) \wedge (\forall j < \ell \leq i : (\sigma, \ell) \models \varphi_1).
 \end{aligned}$$

Nous écrivons $\sigma \models \varphi$ lorsque $(\sigma, 0) \models \varphi$. Ainsi, la notion de satisfaisabilité demeure inchangée pour le fragment standard de LTL. De plus, les opérateurs du passé fonctionnent de la même façon que ceux du futur, mais dans la direction opposée (à l'exception du fait qu'il n'y pas de position avant 0).

Pour chacune des formules suivantes, donnez une formule équivalente qui n'utilise pas les opérateurs du passé:

- (a) $G(p \rightarrow X^{-1}q)$
- (b) $GF^{-1}p$
- (c) $F(q \wedge G^{-1}(p \vee q))$
- (d) $G(p \rightarrow F^{-1}q)$