IGL502/752 – Techniques de vérification et de validation

Université de Sherbrooke

Devoir 2

Enseignant:	Michael Blondin
Date de remise:	mardi 1er octobre 2024 à 13h29
À réaliser:	à deux ou individuellement au 1er cycle individuellement aux cycles supérieurs
Modalités:	remettre en ligne sur Turnin
Bonus:	les questions bonus sont indiquées par ★
Pointage:	sur 30 points au 1er cycle sur 38 points aux cycles supérieurs

Pour tout mot infini $\sigma \in \Sigma^\omega$, nous écrivons inf(σ) pour dénoter l'ensemble des lettres qui apparaissent infiniment souvent dans σ. Par exemple, inf$(abc^\omega) = \{c\}$, inf$(c(bba)^\omega) = \{a, b\}$ et inf$((abc)^\omega) = \{a, b, c\}$.

Question 1. 7,5 pts

Soit $\Sigma \coloneqq \{a, b, c\}$. Pour chaque langage $L_i \subseteq \Sigma^\omega$ ci-dessous, donnez une expression ω-régulière s_i telle que $\mathcal{L}(s_i) = L_i$. Donnez également un mot appartenant à L_i et un mot n'appartenant pas à L_i.

(a) $L_1 \coloneqq \{\sigma \in \Sigma^\omega : \text{inf}(\sigma) = \{a, b, c\}\}$;

(b) $L_2 \coloneqq \{\sigma \in \Sigma^\omega : b \in \text{inf}(\sigma) \land \sigma \text{ contient au moins un } a\}$;

(c) $L_3 \coloneqq \{\sigma \in \Sigma^\omega : \underbrace{\forall i \in \mathbb{N}\ [((\sigma(i) = b) \rightarrow i \text{ est pair}) \land ((\sigma(i) = a) \rightarrow i \text{ est impair})]}_{\text{« la lettre } b \text{ (resp. } a\text{) peut seulement apparaître aux positions paires (resp. impaires) »}}\}$.

Question 2. 7,5 pts

Soit $\Sigma \coloneqq \{a, b, c\}$. Pour chaque langage $L_i \subseteq \Sigma^\omega$ ci-dessous, donnez un automate de Büchi $\mathcal{A}_i$ tel que $\mathcal{L}(\mathcal{A}_i) = L_i$. Dites également si $\mathcal{A}_i$ est déterministe ou non.

(a) $L_1 \coloneqq \{\sigma \in \Sigma^\omega : \text{inf}(\sigma) = \{a, b, c\}\}$;

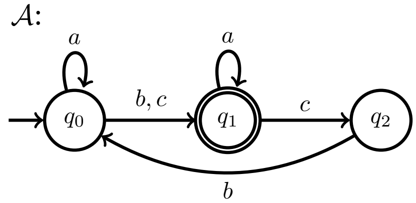
(b) $L_2 \coloneqq \{\sigma \in \Sigma^\omega : \text{si } a \in \text{inf}(\sigma), \text{alors } b \in \text{inf}(\sigma)\}$;

(c) $L_3 \coloneqq \{\sigma \in \Sigma^\omega : \underbrace{\forall i, k \in \mathbb{N}\ [(i < k \land \sigma(i) = a \land \sigma(k) = c) \rightarrow (\exists j \in \mathbb{N} : i < j < k \land \sigma(j) = b)]}_{\text{« si un } c \text{ apparaît après un } a\text{, alors il y a au moins un } b \text{ entre »}}\}$.

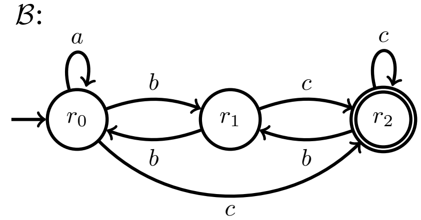
Question 3. 5 pts

Soient $\mathcal{A}$ et $\mathcal{B}$ les automates de Büchi ci-dessous. Construisez l'automate de Büchi $\mathcal{A} \cap \mathcal{B}$ tel que $\mathcal{L}(\mathcal{A} \cap \mathcal{B}) = \mathcal{L}(\mathcal{A}) \cap \mathcal{L}(\mathcal{B})$. Dites si $\mathcal{A}$ et $\mathcal{B}$ acceptent un mot en commun à l'aide de $\mathcal{A} \cap \mathcal{B}$. Justifiez à l'aide de la procédure de détection linéaire de lasso par parcours post-ordre.

$\mathcal{A}$:



$\mathcal{B}$:



Question 4. 10 pts

Soient $AP \coloneqq \{p, q\}$ et $\Sigma \coloneqq 2^{AP}$. Pour chaque formule φ_i ci-dessous, donnez un automate de Büchi $\mathcal{A}_i$ tel que $\mathcal{L}(\mathcal{A}_i) = [\![\varphi_i]\!]$. Donnez également un mot accepté par $\mathcal{A}_i$ et un mot refusé par $\mathcal{A}_i$.

(a) $\varphi_1 = (\mathsf{F}p) \rightarrow (\mathsf{G}q)$;

(b) $\varphi_2 = \neg\mathsf{FG}(\neg p \vee \neg q)$;

(c) $\varphi_3 = p \;\mathsf{U}\; (p \wedge (q \;\mathsf{U}\; \neg p))$;

(d) $\varphi_4 = \mathsf{G}((\mathsf{X}p) \;\mathsf{U}\; q)$.

Vous n'avez pas à répondre à la question ci-dessous si vous êtes au premier cycle. Si vous y répondez, vous pourrez obtenir jusqu'à 1 point bonus.

Question 5. (cycles supérieurs)

Il existe plusieurs autres types d'automates sur les mots infinis: de Muller, Rabin, Street, parité, etc. Explorons l'un de ces formalismes. Un *automate de Muller* est un quintuplet $\mathcal{M} = (Q, \Sigma, \delta, Q_0, F)$ où les quatre premières composantes sont comme celles d'un automate de Büchi, mais où F est une collection d'ensembles d'états plutôt qu'un seul ensemble d'états, c.-à-d. $F \subseteq 2^Q$. Nous disons que $\mathcal{M}$ accepte un mot infini $\sigma \in \Sigma^\omega$ s'il peut lire σ de telle sorte que les états visités infiniment souvent correspondent *précisément* à un ensemble $A \in F$.

(a) Donnez un automate de Muller *déterministe* qui accepte $(a + b)^* a^\omega$, c.-à-d. le langage des mots qui possèdent un nombre fini de b. 3 pts

(b) Montrez que les automates de Muller (non déterministes) sont aussi expressifs que les automates de Büchi (non déterministes), en expliquant comment convertir un automate de Muller vers un automate de Büchi et vice-versa (sans vous souciez de l'efficacité des transformations). 5 pts

Indice: remarquez que $\mathcal{L}(\mathcal{M}) = \bigcup_{A \in F} \mathcal{L}(Q, \Sigma, \delta, Q_0, \{A\})$ *et exploitez le non déterminisme.*

★ Question 6. (bonus pour tous les cycles)

Considérez le système concurrent suivant constitué de deux processus partageant les variables entières x, y, z: ★ 1 pt

$x, y, z \leftarrow 0$
lancer `processus(0)` et `processus(1)` de façon concurrente

`processus(`i`)` *:*
  boucler
1 $x \leftarrow i + y$
2 **si** $(x \neq 1 + i) \wedge (y \neq x)$ **alors aller à** 1
3 $z \leftarrow i$
4 **tant que** $x \cdot z \neq z$ **faire rien**
5 **si** $y = 0$ **alors** $y \leftarrow z - i$
6 $y \leftarrow i + 1$
7 **si** $z = x - y$ **alors aller à** 1
8 `/* section critique */`

Donnez un chemin fini du système qui atteint un état où `processus`(0) et `processus`(1) sont tous deux dans leur section critique. Vous pouvez supposer que $-4 \leq x, y, z < 4$ et que les opérations arithmétiques n'engendrent pas de débordement (le système satisfait cette propriété; elle a déjà été vérifiée).