IGL502/752 – Techniques de vérification et de validation

Université de Sherbrooke

Examen final

Enseignant: Michael Blondin
Date: vendredi 16 décembre 2022
Durée: 3 heures

Directives:

— Vous devez répondre aux questions dans le **cahier de réponses**, et non sur ce questionnaire;

— **Une seule feuille** de notes au format 8½" × 11" est permise;

— **Aucun matériel additionnel** (notes de cours, fiches récapitulatives, etc.) n'est permis;

— **Aucun appareil électronique** (calculatrice, téléphone, montre intelligente, etc.) n'est permis;

— Vous devez donner **une seule réponse** par sous-question;

— L'examen comporte **6 questions** sur **6 pages** valant un total de **50 points**;

— La correction se base notamment sur la **clarté**, l'**exactitude** et la **concision** de vos réponses, ainsi que sur la **justification** pour les questions qui en requièrent une.

Question 1: logique temporelle linéaire (LTL)

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

$$\varphi_1 \coloneqq (p \wedge r)\ \mathsf{U}\ (\mathsf{X}q) \qquad \varphi_2 \coloneqq (\mathsf{GF}q) \wedge (\mathsf{GF}r) \qquad \varphi_3 \coloneqq \mathsf{F}(q \wedge \mathsf{G}(\neg p))$$

(a) Pour chaque formule φ_i, donnez un mot σ_i qui la satisfait et qui ne satisfait pas les deux autres, c.-à-d. 6 pts

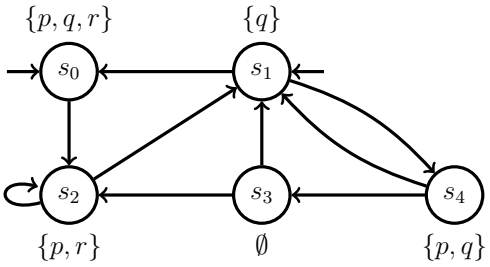
$$\begin{array}{lll} \sigma_1 \models \varphi_1 & \sigma_1 \not\models \varphi_2 & \sigma_1 \not\models \varphi_3, \\ \sigma_2 \not\models \varphi_1 & \sigma_2 \models \varphi_2 & \sigma_2 \not\models \varphi_3, \\ \sigma_3 \not\models \varphi_1 & \sigma_3 \not\models \varphi_2 & \sigma_3 \models \varphi_3. \end{array}$$

1. $\emptyset\{p, q\}^\omega$
2. $(\{p, q\}\{p, r\})^\omega$
3. $\{q\}\emptyset^\omega$

(b) Donnez un mot σ qui satisfait à la fois φ_1, φ_2 *et* φ_3, c.-à-d. tel que $\sigma \models \varphi_1$, $\sigma \models \varphi_2$ et $\sigma \models \varphi_3$. 2 pts

$\{q, r\}^\omega$

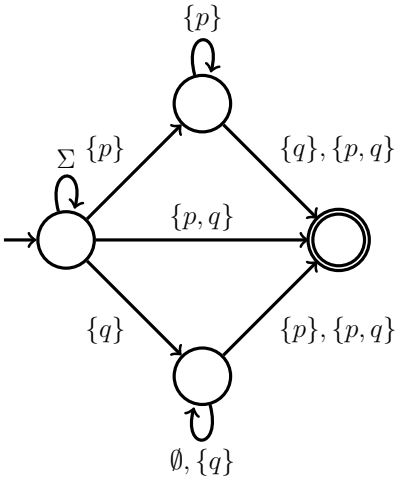
(c) Pour chaque formule φ_i, dites si la structure de Kripke $\mathcal{T}$ ci-dessous satisfait φ_i. Justifiez. 3 pts



1. Non, trace$(s_0\, s_2^\omega)$ enfreint la formule car Xq n'est jamais satisfait.
2. Non, trace$(s_0\, s_2^\omega)$ enfreint la formule car q n'est satisfait qu'une fois.
3. Non, trace$(s_0\, s_2^\omega)$ enfreint la formule car p demeure toujours vrai.

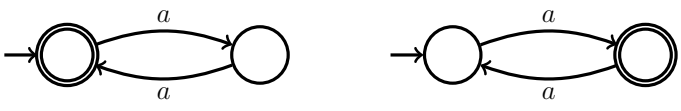
Question 2: automates de Büchi

(a) Donnez un automate de Büchi $\mathcal{B}$ tel que $\mathcal{L}(\mathcal{B}) = [\![\mathsf{F}((p\ \mathsf{U}\ q) \wedge (\mathsf{F}p))]\!]$ sur alphabet $\Sigma \coloneqq \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$. 4 pts



(b) Rappelons que selon la construction vue en classe, les états de l'automate, résultant de l'intersection de deux automates de Büchi $\mathcal{A}$ et $\mathcal{B}$, sont de la forme (p, q, I) où p est un état de $\mathcal{A}$, q est un état de $\mathcal{B}$, et $I \in \{\mathcal{A}, \mathcal{B}\}$. Expliquez pourquoi la troisième composante est nécessaire dans cette construction. 2 pts

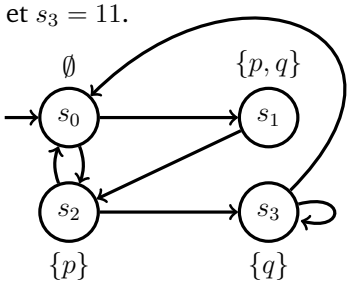
Elle sert à indiquer le prochain automate qui doit visiter un état acceptant. C'est nécessaire car $\mathcal{A}$ et $\mathcal{B}$ ne visitent pas forcément leurs états acceptants aux mêmes moments, par ex. aux moments pairs et impairs pour ces automates qui acceptent le même langage:



Question 3: logique temporelle arborescente (CTL) et vérification symbolique

Rappel: l'abbréviation « BDD » réfère à « diagramme de décision binaire (ordonné et réduit) ».

Supposons que chaque état de la structure de Kripke $\mathcal{T}$ ci-dessous soient codés par la représentation binaire de son indice: $s_0 = 00$, $s_1 = 01$, $s_2 = 10$ et $s_3 = 11$.

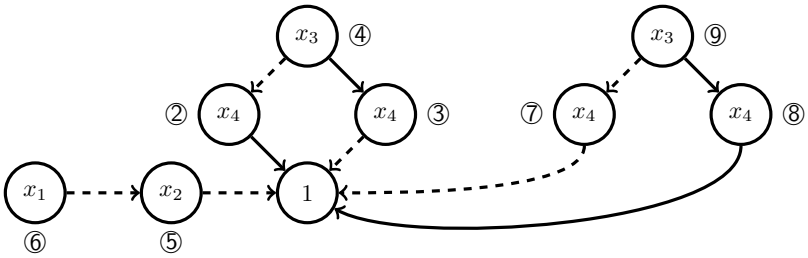


(a) Pour chaque formule Φ ci-dessous, donnez l'ensemble $[\![\Phi]\!]$ des états de $\mathcal{T}$ qui satisfont Φ. 6 pts

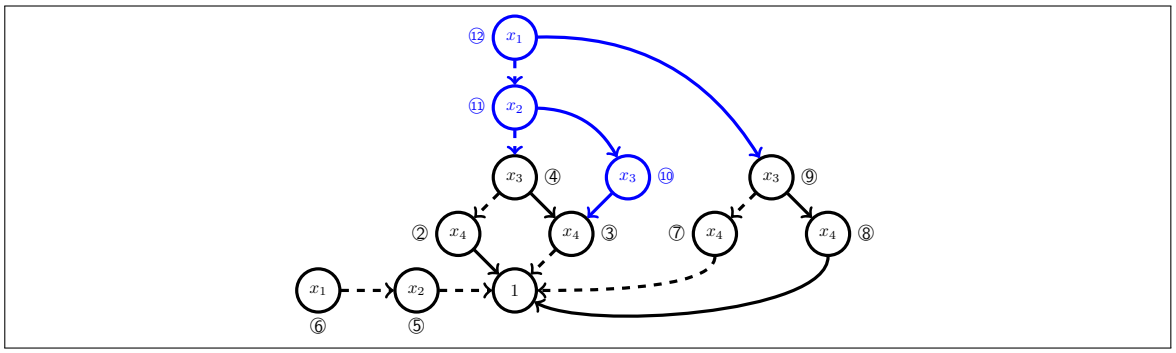
(i) $\forall \mathsf{F}\, \exists \mathsf{G} \neg q$ (ii) $\exists (p \,\mathsf{U}\, q)$ (iii) $\forall \mathsf{X}\, \exists (p \,\mathsf{U}\, q)$

(i) $\{s_0, s_1, s_2\}$ (ii) $\{s_1, s_2, s_3\}$ (iii) $\{s_0, s_1\}$

(b) Considérons le BDD ci-dessous sur variables $x_1 < x_2 < x_3 < x_4$. Le sommet 6 représente $I = \{s_0\}$ codé sur variables x_1x_2. Le sommet 4 représente $[\![p]\!] = \{s_1, s_2\}$ codé sur variables x_3x_4. Complétez le BDD afin d'obtenir un sommet qui représente l'ensemble des transitions $\rightarrow = \{s_0s_1, s_0s_2, \ldots\}$ sur variables $x_1x_2x_3x_4$. 4 pts



Remarques: omettez le sommet 0; et il n'est pas obligatoire d'appliquer un algorithme.



(c) Expliquez comment vérifier algorithmiquement $\mathcal{T} \models \exists \mathsf{X} p$ à partir du BDD construit en (b) et ces opérations: 2 pts

Opération	**Entrées**	**Sortie**
$\texttt{apply}_{\bigcirc}(u, v)$	sommets u et v	sommet w qui représente $f_u \circ f_v$
$\texttt{exists}(u, i)$	sommet u et indice i	sommet w qui représente $\exists x_i \in \{0, 1\} : f_u$

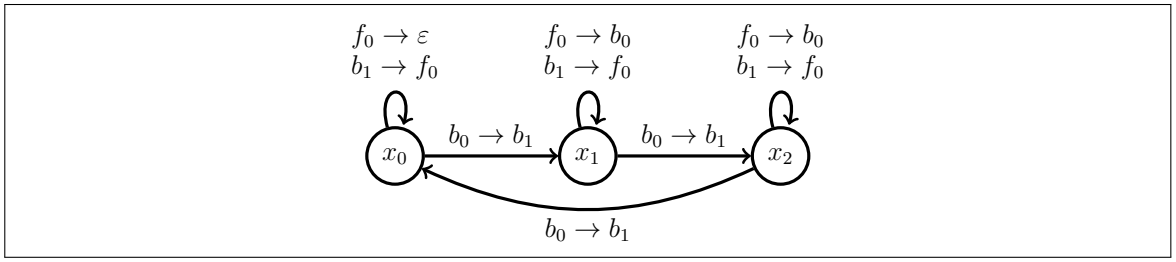
On teste $\texttt{apply}_{\rightarrow}(⑥, \texttt{exists}(\texttt{exists}(\texttt{apply}_{\wedge}(⑫, ④), 3), 4)) = ①$.

Question 4: systèmes à pile

Considérons ce programme constitué de deux fonctions et d'une variable entière globale x qui n'excède jamais 2:

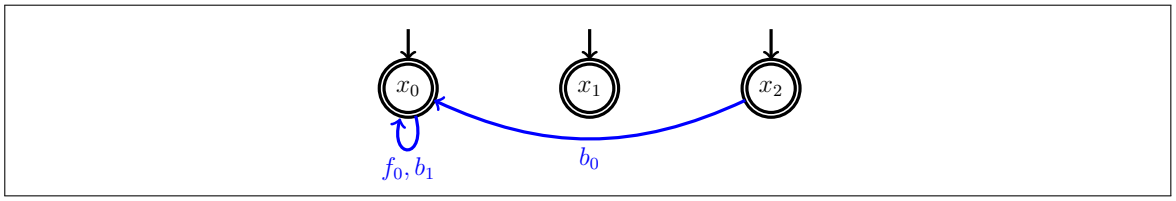
```
        var x ∈ {0, 1, 2}

        foo():                      bar():
f0:       si x > 0:           b0:     x = (x + 1) mod 3
            bar()             b1:     foo()
```

(a) Modélisez le programme avec un système à pile $\mathcal{P}$. 3 pts



(b) Construisez partiellement un $\mathcal{P}$-automate $\mathcal{B}$ qui accepte $\text{Pre}^*(\mathit{Conf}(\mathcal{A}))$, où $\mathcal{A}$ est ce $\mathcal{P}$-automate: 3 pts

Plus précisément, ajoutez *trois transitions* en exécutant l'algorithme de saturation vu en classe.

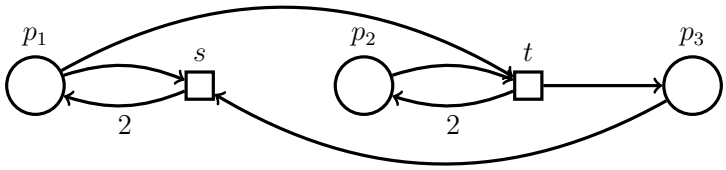


(c) Supposons que l'on ait complété $\mathcal{B}$ en (b). Comment peut-on déterminer les valeurs de x à partir desquelles le programme termine? 1 pt

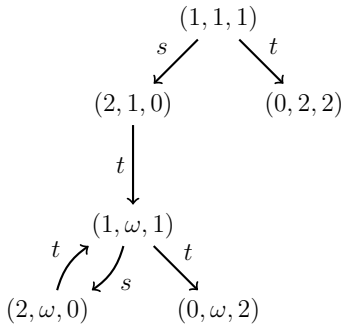
Le programme termine sur entrée $x = i$ ssi $\langle x_i, f_0 \rangle \in \mathit{Conf}(\mathcal{B})$. Il suffit donc de vérifier, pour chaque $i \in [0..2]$, s'il existe une transition étiquetée par f_0 qui quitte l'état x_i dans $\mathcal{B}$.

Question 5: réseaux de Petri

Soit le réseau de Petri $\mathcal{N} = (P, T, F)$ suivant:



(a) Dessinez un graphe de couverture qui débute en $\boldsymbol{m} \coloneqq (1,1,1)$. 3 pts



(b) Dites lesquels de ces marquages peuvent être couverts à partir de $\boldsymbol{m} \coloneqq (1,1,1)$. Justifiez brièvement. 1,5 pts

$$\boldsymbol{m}_0 \coloneqq (1,1,2), \qquad \boldsymbol{m}_1 \coloneqq (0,3,2), \qquad \boldsymbol{m}_2 \coloneqq (4,2,0).$$

0. Non, car les marquages du graphe qui possède une valeur ≥ 2 dans p_3 ont 0 dans p_1.
1. Oui, car $(0,\omega,2) \geq (0,3,2)$.
2. Non, car aucun marquage du graphe possède une valeur ≥ 4 dans p_1.

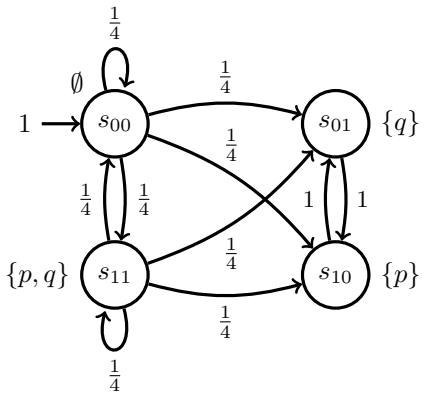
(c) L'ensemble des marquages qui peuvent couvrir $\boldsymbol{m}' \coloneqq (1,1,0)$ est $\uparrow\boldsymbol{m}'$. Pourquoi? 2,5 pts

Parce que l'algorithme arrière n'ajoute rien à sa base à partir de $\uparrow\boldsymbol{m}'$:

$$(1,1,0)_s = (1,1,1)$$
$$(1,1,0)_t = (2,1,0)$$

Question 6: chaînes de Markov

Considérons un système constitué de deux processus. Chaque processus i possède une variable booléenne x_i. On aimerait qu'à partir d'un certain moment, ce soit toujours le cas que $x_2 = \neg x_1$. Afin d'accomplir cette tâche, les processus modifient leurs variables de façon probabiliste, comme suit (où s_{ab} désigne $x_1 = a$ et $x_2 = b$):



Remarque: il n'est pas obligatoire d'appliquer des algorithmes pour répondre aux questions.

(a) Dites si la chaîne de Markov $\mathcal{M}$ ci-dessus satisfait $\mathcal{P}_{\geq 3/4}((\neg p)\ \mathsf{U}^{\leq 2}\ q)$. Justifiez. 2 pts

Sol. 1. Non. Pour satisfaire $(\neg p)\ \mathsf{U}^{\leq 2}\ q$, il faut que s_{00} atteigne $\{s_{01}, s_{11}\}$ en une étape, ou qu'il boucle sur lui-même, puis atteigne $\{s_{01}, s_{11}\}$ en une étape. Ainsi,

$$\mathbb{P}(s_{00} \models (\neg p)\ \mathsf{U}^{\leq 2}\ q) = 1/2 + 1/4 \cdot 1/2 = 5/8 < 6/8 = 3/4.$$

Sol. 2. Non. Les chemins qui satisfont $(\neg p)\ \mathsf{U}^{\leq 2}\ q$ sont

$$s_{00} \xrightarrow{\frac{1}{4}} s_{01},\ s_{00} \xrightarrow{\frac{1}{4}} s_{11},\ s_{00} \xrightarrow{\frac{1}{4}} s_{00} \xrightarrow{\frac{1}{4}} s_{01} \text{ et } s_{00} \xrightarrow{\frac{1}{4}} s_{00} \xrightarrow{\frac{1}{4}} s_{11}.$$

Ainsi, $\mathbb{P}(s_{00} \models (\neg p)\ \mathsf{U}^{\leq 2}\ q) = 1/4 + 1/4 + 1/16 + 1/16 = 10/16 < 12/16 = 3/4$.

(b) Dites si la chaîne de Markov $\mathcal{M}$ ci-dessus satisfait $\mathcal{P}_{=1}(\mathsf{F}\,\mathcal{P}_{=1}(\mathsf{G}\,(p \to \mathcal{P}_{=1}(\mathsf{X}\,q))))$. Justifiez. 3 pts

Rappel: $\mathcal{P}_{=1}(\mathsf{G}\Phi) \equiv \mathcal{P}_{=0}(\mathsf{F}\neg\Phi)$.

Oui, la propriété est satisfaite à partir de tous les états car

$$\begin{aligned}
&[\![\mathcal{P}_{=1}(\mathsf{F}\,\mathcal{P}_{=1}(\mathsf{G}\,(p \to \mathcal{P}_{=1}(\mathsf{X}\,q))))]\!] \\
&[\![\mathcal{P}_{=1}(\mathsf{F}\,\mathcal{P}_{=0}(\mathsf{F}\,(p \wedge \neg\mathcal{P}_{=1}(\mathsf{X}\,q))))]\!] \\
&[\![\mathcal{P}_{=1}(\mathsf{F}\,\mathcal{P}_{=0}(\mathsf{F}\,(\{s_{11}, s_{10}\} \cap \overline{\{s_{10}\}})))]\!] \\
&= [\![\mathcal{P}_{=1}(\mathsf{F}\,\mathcal{P}_{=0}(\mathsf{F}\,s_{11}))]\!] \\
&= [\![\mathcal{P}_{=1}(\mathsf{F}\,\{s_{01}, s_{10}\})]\!] \\
&= \{s_{00}, s_{01}, s_{10}, s_{11}\} \qquad \text{(car unique CFC terminale)}.
\end{aligned}$$

(c) Spécifiez cette propriété en PCTL: « à partir d'un certain moment, ceci demeure vrai: $x_2 = \neg x_1$ ». 2 pts

$\mathcal{P}_{=1}(\mathsf{F}\,\mathcal{P}_{=1}(\mathsf{G}\,(p \oplus q)))$