IGL502/752 – Techniques de vérification et de validation

Université de Sherbrooke

Examen final

Enseignant: Michael Blondin
Date: vendredi 17 décembre 2021
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)

Soient $AP \coloneqq \{p, q\}$ et les formules LTL suivantes sur AP, où « $\oplus$ » dénote l'opération « OU exclusif »:

$$\varphi_1 \coloneqq \neg\mathsf{FG}(p \land q) \qquad \varphi_2 \coloneqq p \,\mathsf{U}\, (p \oplus q) \qquad \varphi_3 \coloneqq \mathsf{XX}q \lor \mathsf{G}(p \rightarrow \mathsf{F}\neg p)$$

(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

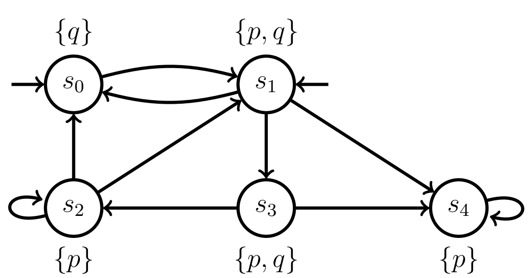
$$\begin{array}{lll} \sigma_1 \models \varphi_1 & \sigma_1 \not\models \varphi_2 & \sigma_1 \not\models \varphi_3, \\ \sigma_2 \not\models \varphi_1 & \sigma_2 \models \varphi_2 & \sigma_2 \not\models \varphi_3, \\ \sigma_3 \not\models \varphi_1 & \sigma_3 \not\models \varphi_2 & \sigma_3 \models \varphi_3.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

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

(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

$\{q\}\{q\}\{q\}\emptyset^\omega$

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



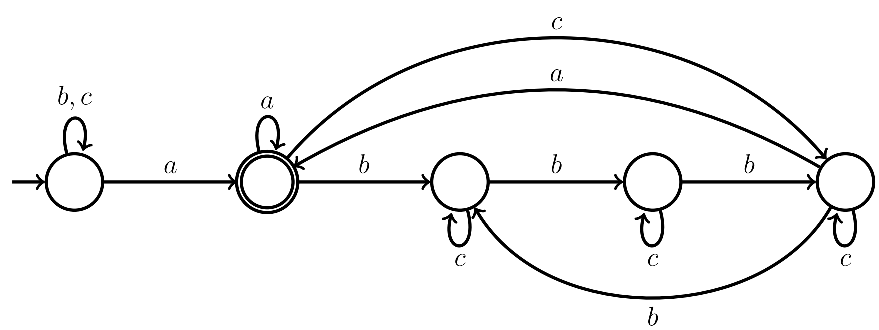
1. Oui: seuls s_1 et s_3 satisfont $p \wedge q$, et ils n'induisent aucun cycle.
2. Oui: tous les états satisfont $p \vee q$, et par 1. on sait qu'on doit éventuellement satisfaire $p \oplus q$.
3. Non: trace$(s_0\, s_1\, s_4^\omega)$ enfreint la formule.

Question 2: langages ω-réguliers

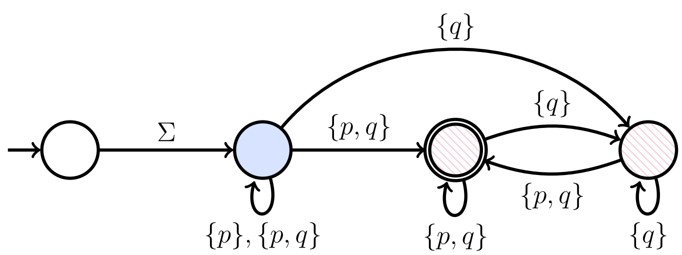
(a) Donnez une expression ω-régulière ***ou*** un automate de Büchi pour ce langage: 3 pts

$$L := \{\sigma \in \{a,b,c\}^\omega : \overbrace{[\forall i \in \mathbb{N}\ \exists j \geq i : \sigma(j) = a]}^{\sigma \text{ contient une infinité de } a} \wedge \underbrace{[\forall i, k \in \mathbb{N} : (\sigma(i) = a \wedge i < k \wedge \sigma(k) = a) \rightarrow |\{j \in [i..k] : \sigma(j) = b\}| \bmod 3 = 0]}_{\text{le nombre de } b \text{ entre chaque paire de } a \text{ est un multiple de } 3}\}.$$

$(b + c)^*(a(c + bc^*bc^*b)^*)^\omega$ ou



(b) Donnez un automate de Büchi $\mathcal{B}$ tel que $\mathcal{L}(\mathcal{B}) = [\![\mathsf{X}(p\ \mathsf{U}\ (\mathsf{G}q)) \wedge \mathsf{GF}p]\!]$ sur alphabet $\Sigma := \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$. 3 pts

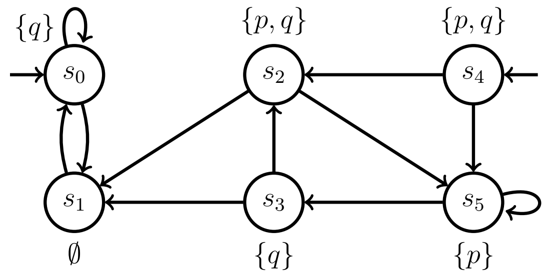


(Explication: l'état initial gère X; l'état entièrement coloré gère p; et les deux états hachurés gèrent $\mathsf{G}q$ et $\mathsf{GF}p$.)

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 soit codé par la représentation binaire de son indice: $s_0 = 000$, $s_1 = 001$, $s_2 = 010$, $s_3 = 011$, $s_4 = 100$ et $s_5 = 101$ (les autres chaînes sont invalides).



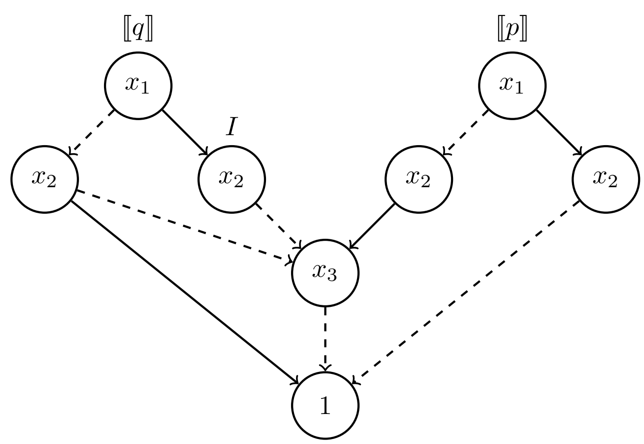
(a) Pour chaque formule Φ ci-dessous, donnez l'ensemble $[\![\Phi]\!]$ des états de $\mathcal{T}$ qui satisfont Φ, et dites si $\mathcal{T} \models \Phi$. 6 pts

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

(i) Non: $\{s_0, s_1, s_2, s_3\}$ (ii) Oui: $\{s_0, s_2, s_3, s_4\}$ (iii) Oui: $\{s_0, \ldots, s_5\}$

(b) Donnez un BDD qui représente les états initiaux I, l'ensemble $[\![p]\!]$ et l'ensemble $[\![q]\!]$. Indiquez clairement quels sommets du BDD correspondent à ces trois ensembles. 4 pts

Remarque: il n'est pas obligatoire d'appliquer un algorithme.



(c) Expliquez comment vérifier algorithmiquement si $\mathcal{T} \models p \land q$ à partir du BDD construit en (b). 2 pts

On obtient $x \coloneqq \mathtt{apply}_\land([\![p]\!], [\![q]\!])$ et $y \coloneqq \mathtt{apply}_\to(I, x)$, puis on teste si $y = 1$.

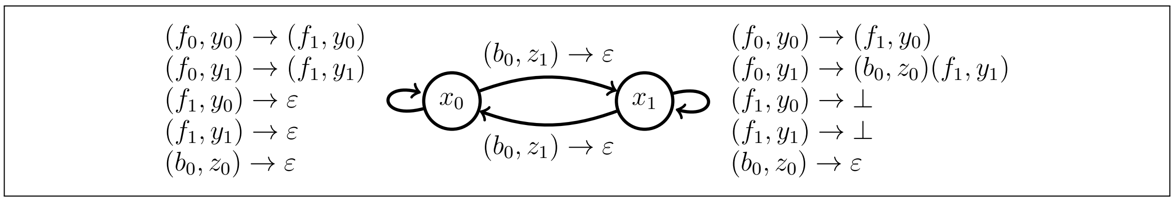
Question 4: systèmes à pile

Considérons ce programme constitué de deux fonctions et d'une variable booléenne globale x:

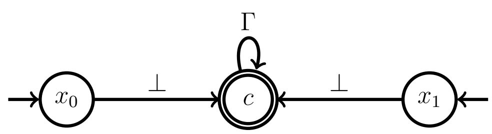
```
      bool x ∈ {faux, vrai}

      foo(bool y):                    bar(bool z):
f0:     tant que x ∧ y:          b0:    x = x ⊕ z
          bar(¬y)

f1:     assert(¬x)
```

Remarque: l'absence d'étiquette dans le corps de la boucle « tant que » est volontaire; supposez que le corps est exécuté au même moment qu'une évaluation à « vrai » de la condition en f_0.

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

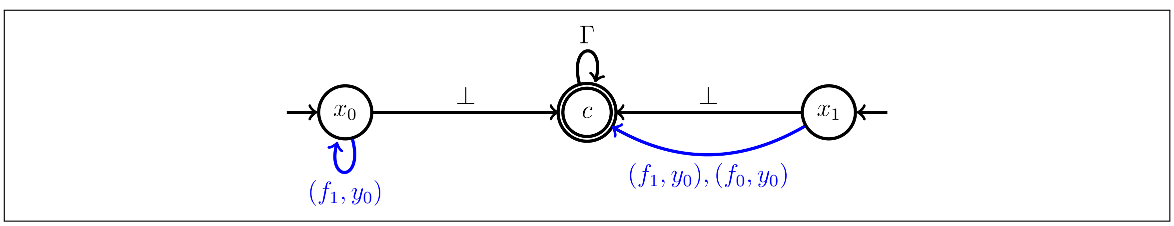


(b) Construisez partiellement un $\mathcal{P}$-automate $\mathcal{B}$ qui accepte $\text{Pre}^*(\mathit{Conf}(\mathcal{A}))$, où $\mathcal{A}$ est ce $\mathcal{P}$-automate: 3 pts



Plus précisément, ajoutez *au moins trois nouvelles transitions* à $\mathcal{A}$ en exécutant l'algorithme de saturation vu en classe. Au moins deux de ces transitions doivent être obtenues *sans* utiliser une transition de $\mathcal{P}$ étiquetée par une règle de la forme « *lettre* $\to \varepsilon$ ».

Rappel: Γ *est l'alphabet de* $\mathcal{P}$.

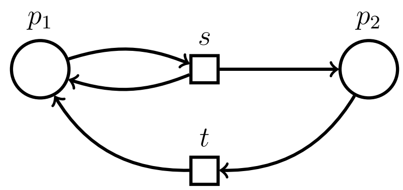


(c) Supposons que l'on ait complété $\mathcal{B}$ en (b). Si $(f_0, y_i) \in \mathit{Conf}(\mathcal{B})$, que peut-on conclure sur l'assertion? 1 pt

L'assertion peut être enfreinte lorsqu'on appelle `foo(i)`.

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 $\boldsymbol{m} := (0, 1)$. Décrivez l'ensemble des marquages couvrables à partir de $\boldsymbol{m}$. 2,5 pts

> Tous les marquages car on obtient (ω, ω):
>
> $$(0,1) \xrightarrow{\quad t \quad} (1,0) \xrightarrow{\quad s \quad} (\omega, \omega) \circlearrowleft s, t$$

(b) Exécutez l'algorithme arrière afin de déterminer l'ensemble des marquages qui peuvent couvrir $\boldsymbol{m}' := (0, 1)$, c'est-à-dire $\uparrow\text{Pre}^*(\uparrow\boldsymbol{m}')$. 3 pts

On obtient $\mathbb{N}^2 \setminus \{(0, 0)\}$:

Itér.	**Base**	**Marquages obtenus**	
0	$\{(0,1)\}$	$(0,1)_s = (1,0)$	$(0,1)_t = (0,2)$
1	$\{(0,1),(1,0)\}$	$(1,0)_s = (1,0)$	$(1,0)_t = (0,1)$

(c) Dites lesquels de ces marquages peuvent couvrir $\boldsymbol{m}' = (0, 1)$. Justifiez brièvement. 1,5 pts

$$\boldsymbol{m}_0 := (0,1), \qquad \boldsymbol{m}_1 := (3,0), \qquad \boldsymbol{m}_2 := (0,0).$$

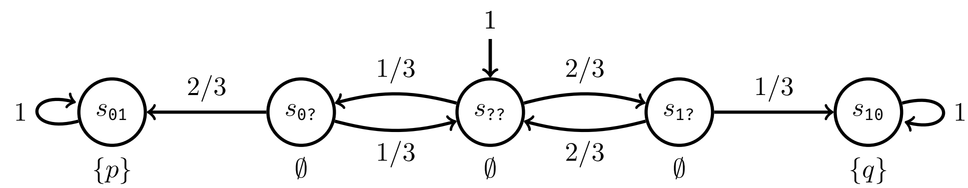
> Tous les marquages sauf $(0, 0)$ sont plus supérieurs ou égaux à $(0, 1)$ ou $(1, 0)$, donc: $\boldsymbol{m}_0$ et $\boldsymbol{m}_1$.

Question 6: chaînes de Markov

Considérons une pièce de monnaie biaisée qui retourne pile avec probabilité $1/3$ et face avec probabilité $2/3$. Cet algorithme cherche à simuler une pièce non biaisée à l'aide d'une pièce biaisée:

répéter
  choisir un bit x à pile ou face avec la pièce biaisée
  choisir un bit y à pile ou face avec la pièce biaisée
jusqu'à $x \neq y$
si $x = 0$ **alors** **retourner** *pile*
sinon **retourner** *face*

L'algorithme peut être modélisé à l'aide de la chaîne de Markov $\mathcal{M}$ ci-dessous, où p et q correspondent respectivement à « pile » et « face ». On aimerait donc que $\mathcal{M}$ satisfasse la propriété PCTL $\varphi := \mathcal{P}_{=1/2}(\mathsf{F}\, p) \land \mathcal{P}_{=1/2}(\mathsf{F}\, q)$.



(a) La chaîne de Markov $\mathcal{M}$ satisfait φ. Expliquez pourquoi. 4 pts

Comme on atteint une CFC terminale avec probabilité 1, il suffit de confirmer que $\mathbb{P}(s_{\texttt{??}} \models \mathsf{F}p) = 1/2$. On a $S_0 = \{s_{\texttt{10}}\}$, $S_1 = \{s_{\texttt{01}}\}$ et $S_? = \{s_{\texttt{0?}}, s_{\texttt{??}}, s_{\texttt{1?}}\}$. Ainsi:

$$\mathbf{A} = \begin{pmatrix} 0 & 1/3 & 0 \\ 1/3 & 0 & 2/3 \\ 0 & 2/3 & 0 \end{pmatrix} \text{ et } \boldsymbol{b} = \begin{pmatrix} 2/3 \\ 0 \\ 0 \end{pmatrix}.$$

Il faut donc résoudre:

$$\begin{pmatrix} 1 & -1/3 & 0 \\ -1/3 & 1 & -2/3 \\ 0 & -2/3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 2/3 \\ 0 \\ 0 \end{pmatrix}.$$

Par l'affirmation, on devine que $y = 1/2$. Comme $x - y/3 = 2/3$ et $z - 2y/3 = 0$, on obtient $x = 5/6$ et $z = 1/3$, ce qui est bien une solution du système.

Remarque: avec cette information, les calculs devraient être plutôt simples.

(b) Quelle est la valeur de $\mathbb{P}(s_{\texttt{??}} \models \mathsf{G}(\neg p \wedge \neg q))$? Justifiez. 1,5 pts

$$\begin{aligned} \mathbb{P}(s_{\texttt{??}} \models \mathsf{G}(\neg p \wedge \neg q)) &= 1 - \mathbb{P}(s_{\texttt{??}} \models \mathsf{F}(p \vee q)) \\ &= 1 - 1 && \text{(car on atteint une CFC terminale avec proba. 1)} \\ &= 0. \end{aligned}$$

(c) Est-ce que $\mathcal{M}$ satisfait $\mathcal{P}_{\geq 1/3}(\mathsf{X}\,\mathcal{P}_{>0}(\mathsf{X}\,p))$? Justifiez. 1,5 pts

Oui, on a $[\![\mathcal{P}_{>0}(\mathsf{X}\,p)]\!] = \{s_{\texttt{01}}, s_{\texttt{0?}}\}$ et $\mathbb{P}(s_{\texttt{??}} \models \mathsf{X} s_{\texttt{0?}}) = 1/3$.