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 **3 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:

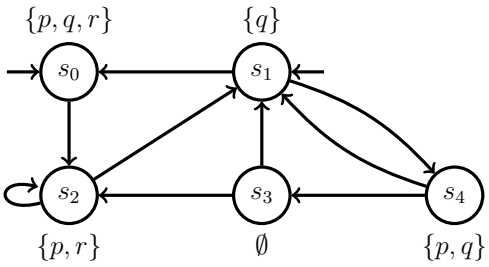
$$\varphi_1 \coloneqq (p \wedge r)\ \mathsf{U}\ (\mathsf{X}q) \qquad \varphi_2 \coloneqq (\mathsf{GF}q) \wedge (\mathsf{GF}r) \qquad \varphi_3 \coloneqq \mathsf{F}(q \wedge \mathsf{G}(\neg p))$$

(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

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

(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

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



Question 2: automates de Büchi

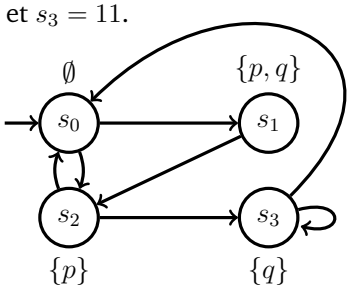
(a) Donnez un automate de Büchi $\mathcal{B}$ tel que $\mathcal{L}(\mathcal{B}) = [\![\mathsf{F}((p\ \mathsf{U}\ q) \wedge (\mathsf{F}p))]\!]$ sur alphabet $\Sigma \coloneqq \{\emptyset, \{p\}, \{q\}, \{p, q\}\}$. 4 pts

(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

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

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

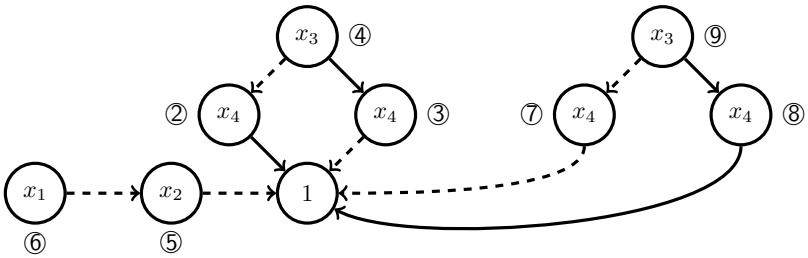
Supposons que chaque état de la structure de Kripke $\mathcal{T}$ ci-dessous soient codés par la représentation binaire de son indice: $s_0 = 00$, $s_1 = 01$, $s_2 = 10$ et $s_3 = 11$.



(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) $\forall \mathsf{X}\, \exists(p\ \mathsf{U}\ q)$

(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 $\exists x_i \in \{0, 1\} : f_u$

Question 4: systèmes à pile

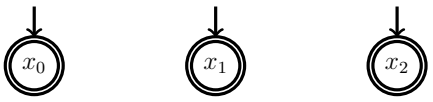
Considérons ce programme constitué de deux fonctions et d'une variable entière globale x qui n'excède jamais 2:

```
    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

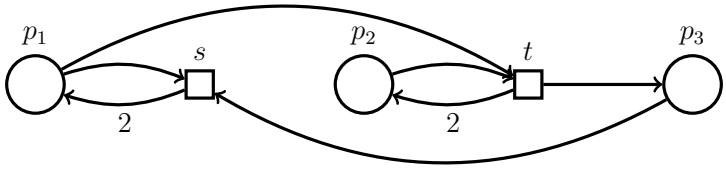


Plus précisément, ajoutez *trois transitions* en exécutant l'algorithme de saturation vu en classe.

(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

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

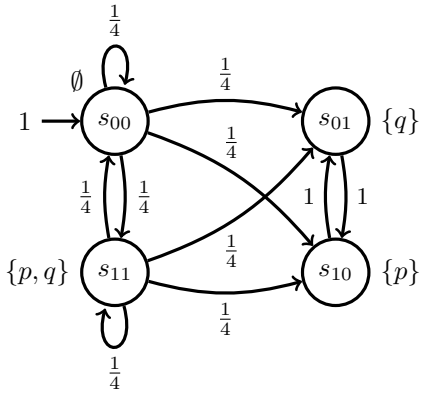
(b) Dites lesquels de ces marquages peuvent être couverts à partir de $\boldsymbol{m} \coloneqq (1, 1, 1)$. Justifiez brièvement. 1,5 pts

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

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

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

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

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

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