Examen – Concepts et Model-Checking

9 mars 2020

Durée: 105 minutes.

1 Logique temporelle linéaire

Soit $AP = \{p, q\}$. Pour les paires de formules suivantes, résoudre ces questions :

- Est-ce que ϕ_1 implique ϕ_2 ? Si ce n'est pas le cas, donner un mot infini sur 2^{AP} qui satisfait ϕ_1 mais pas ϕ_2.
- La même question avec les rôles de ϕ_1 et ϕ_2 inversés.

(a) $\phi_1 = \mathbf{F}\,\mathbf{G}\,(p\,\mathbf{U}\,q)$ et $\phi_2 = \mathbf{F}\,\mathbf{G}\,(\neg p \to q)$;

Solution :

- $\phi_1 \Rightarrow \phi_2$ car $p\,\mathbf{U}\,q \equiv q \vee (p \wedge \mathbf{X}\,(p\,\mathbf{U}\,q))$, du coup $p\,\mathbf{U}\,q \Rightarrow p \vee q \equiv \neg p \to q$.
- $\phi_2 \not\Rightarrow \phi_1$ car $\{p\}^\omega$ est modèle de ϕ_2 mais pas de ϕ_1.

(b) $\phi_1 = \mathbf{G}\,((\mathbf{F}\,p) \to q)$ et $\phi_2 = \mathbf{G}\,(q\,\mathbf{U}\,p)$;

Solution :

- $\phi_1 \not\Rightarrow \phi_2$ car $\{q\}^\omega$ est modèle de ϕ_1 mais pas de ϕ_2.
- $\phi_2 \not\Rightarrow \phi_1$ car $\{p\}^\omega$ est modèle de ϕ_2 mais pas de ϕ_1.

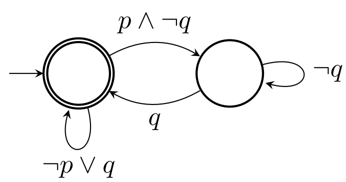
2 Automates de Büchi

Soit encore $AP = \{p, q\}$. Construire des automates de Büchi pour chacune des formules suivantes. (L'utilisation de la construction systématique montrée en cours n'est ni requise ni recommandée.)

(a) $\phi_1 = \mathbf{G}\,(p \to \mathbf{F}\,q)$;

Solution :

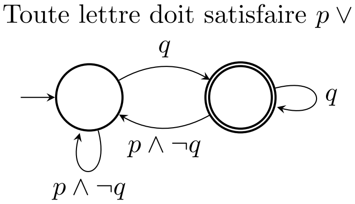
Cet automate était dans les transparents:



(b) $\phi_2 = \mathbf{G}\,(p\,\mathbf{U}\,q)$;

Solution :

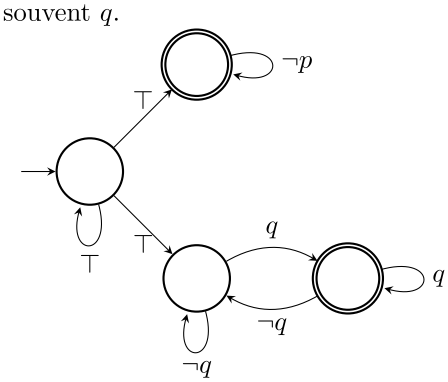
Toute lettre doit satisfaire $p \vee q$ (voir 1a), et il faut q infiniment souvent.



(c) $\phi_3 = (\mathbf{G}\,\mathbf{F}\,p) \to (\mathbf{G}\,\mathbf{F}\,q)$.

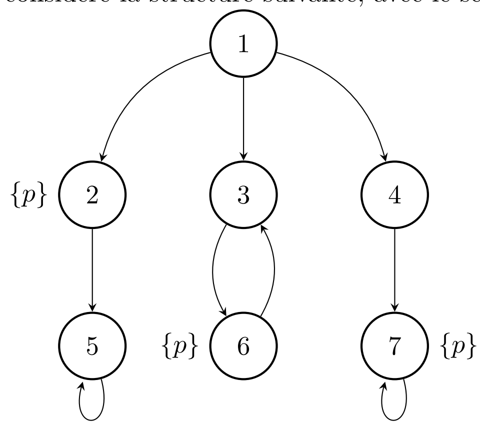
Solution :

La formule est équivalente à $(\mathbf{F}\,\mathbf{G}\,\neg p) \vee (\mathbf{G}\,\mathbf{F}\,q)$, donc finiment souvent p ou infiniment souvent q.



3 CTL

On considère la structure suivante, avec le seul prédicat p, et des formules de CTL.



(a) On a $[\![p]\!] = \{2, 6, 7\}$. Calculer les ensembles suivants:

- $[\![\mathbf{EF}\, p]\!]$ et $[\![\mathbf{AG}\, p]\!]$;
- $[\![\mathbf{AG}\,\mathbf{EF}\, p]\!]$ et $[\![\mathbf{EF}\,\mathbf{AG}\, p]\!]$;
- $[\![\mathbf{EF}\,\mathbf{AG}\,\mathbf{EF}\, p]\!]$ et $[\![\mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\, p]\!]$.

Solution :

- $[\![\mathbf{EF}\, p]\!] = \{1, 2, 3, 4, 6, 7\}$ et $[\![\mathbf{AG}\, p]\!] = \{7\}$;
- $[\![\mathbf{AG}\,\mathbf{EF}\, p]\!] = \{3, 4, 6, 7\}$ et $[\![\mathbf{EF}\,\mathbf{AG}\, p]\!] = \{1, 4, 7\}$;
- $[\![\mathbf{EF}\,\mathbf{AG}\,\mathbf{EF}\, p]\!] = \{1, 3, 4, 6, 7\}$ et $[\![\mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\, p]\!] = \{4, 7\}$.

(b) Prouver ou réfuter (en général !) :

- $\mathbf{EF}\,\mathbf{AG}\, p$ implique $\mathbf{EF}\, p$;
- $\mathbf{AG}\, p$ implique $\mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\, p$.

Solution : Les deux implications sont vraies.

- Un état s satisfaisant $\mathbf{EF}\,\mathbf{AG}\, p$ est à l'origine d'un chemin ménant à un état s' satisfaisant $\mathbf{AG}\, p$, et du coup s' satisfait p aussi.
- Si un état s satisfait $\mathbf{AG}\, p$, alors tous les états accessibles depuis s satisfont $\mathbf{AG}\, p$ et du coup aussi $\mathbf{EF}\,\mathbf{AG}\, p$. Alors s satisfait $\mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\, p$.

(c) (Bonus:) Prouver les propriétés suivantes:

- $\mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\,\mathbf{EF}\, p \equiv \mathbf{AG}\,\mathbf{EF}\, p$;
- $\mathbf{EF}\,\mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\, p \equiv \mathbf{EF}\,\mathbf{AG}\, p$.

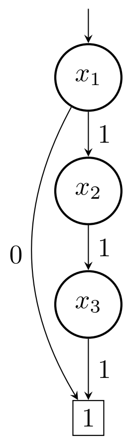
Solution : Rappellons que $\mathbf{EF}\,\mathbf{EF}\, p \equiv \mathbf{EF}\, p$ et $\mathbf{AG}\,\mathbf{AG}\, p \equiv \mathbf{AG}\, p$. Dans les deux cas, pour le sens $\Rightarrow$ il suffit alors d'appliquer le résultat $\mathbf{EF}\,\mathbf{AG}\, p \Rightarrow \mathbf{EF}\, p$ de (b). Pour le sens $\Leftarrow$ il suffit d'utiliser $\mathbf{AG}\, p \Rightarrow \mathbf{AG}\,\mathbf{EF}\,\mathbf{AG}\, p$.

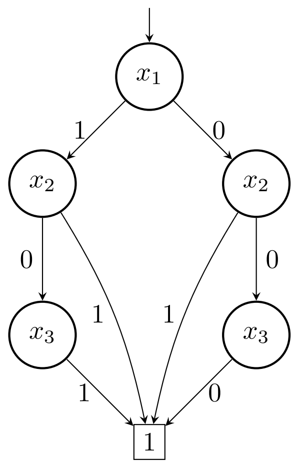
4 Diagrammes de décision binaires

Soient $V := \{x_1, \ldots, x_n\}$, pour $n \geq 1$, des variables booléennes avec l'ordre $x_1 \prec \cdots \prec x_n$. Pour une fonction booléenne f sur V, soit $B(f)$ le nombre de sommets étiquetés par des variables dans le BDD pour f.

(a) Donner les BDD de $f_1 = x_1 \to (x_2 \wedge x_3)$ et $f_2 = (x_1 \leftrightarrow x_3) \vee x_2)$.

Solution :

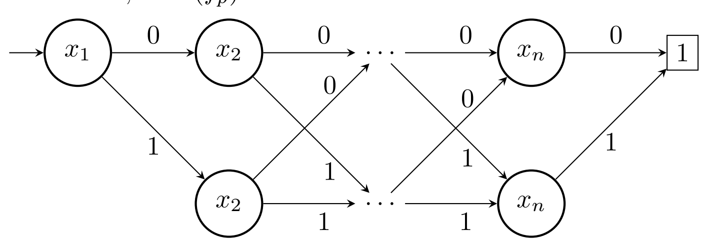




(b) Donner $B(f_p)$ en fonction de n, où f_p est la fonction de parité qui donne 1 ssi V contient un nombre pair de variables qui sont 1.

Solution :

La parité étant la somme modulo 2, tout sommet doit mémoriser la parité des variables précédentes, et $B(f_p) = 2n - 1$.



(c) On note $(x_1 \cdots x_n)_2$ la valeur binaire de V, p.ex. $(1100)_2 = 12$. En fonction de n et i, donner $B(g_i)$, où $i \geq 0$ et $g_i = 1$ ssi $(x_1 \cdots x_n)_2 \geq i$.

Solution :

Les cas intéressants sont $0 < i < 2^n$. Si $i \geq 2^n$, le BDD consisterait simplement du sommet 0, et si $i = 0$, c'est le seul sommet 1.

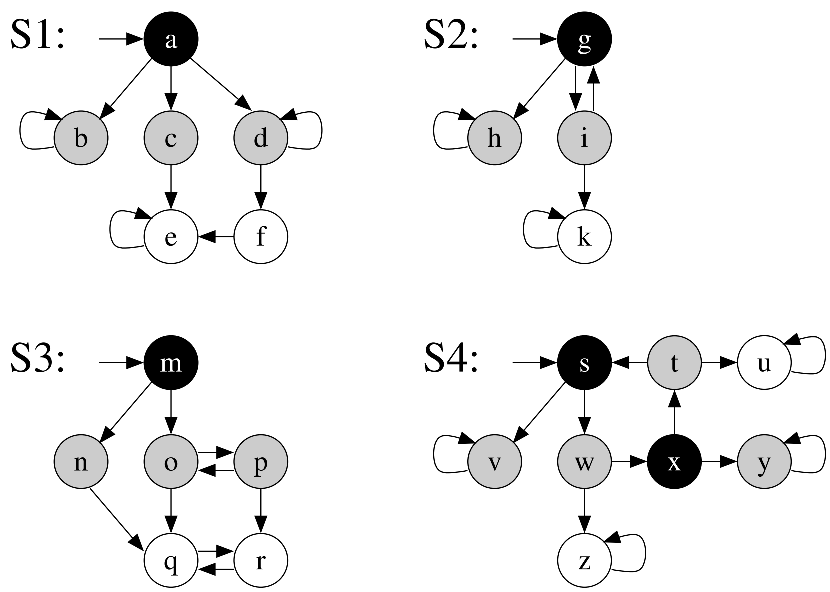
Soit $i = (b_1 \cdots b_n)_2$. On constate que $(x_1 \cdots x_n)_2 \geq (b_1 \cdots b_n)_2$ si soit les deux vecteurs sont égaux, soit il existe k tel que $x_k > b_k$ et pour tout $j < k$, $x_k = b_k$. Du coup, pour $k = 1, \ldots, n$ on compare x_k et b_k: si trouve $x_k > b_k$ on accepte, si $x_k < b_k$ on rejète, et dès qu'il ne reste que des 0 à la fin de $b_1 \cdots b_n$, on accepte aussi.

Soit donc j l'index maximal tel que $b_j = 1$, alors $B(g_i) = j$. Le BDD possède un sommet n_k pour tout x_k, $k = 1, \ldots, j$:

- Si $b_k = 0$, $n_k \xrightarrow{1} 1$ et $n_k \xrightarrow{0} n_{k+1}$.
- Si $b_k = 1$, $n_k \xrightarrow{0} 0$ et $n_k \xrightarrow{1} n_{k+1}$ (avec $n_{k+1} := 1$ si $k = j$).

5 Simulation et bisimulation

On considère les structures S_1, S_2, S_3, S_4 ci-dessous. Les prédicats sont α, β, γ tels que les états en noir satisfont α, les états en gris β, et les états en blanc γ.



(a) Quelles paires de structures sont bisimilaires ? Pour chaque pair, soit exhiber une relation de bisimulation soit une formule CTL qui les distingue.

Solution :

- $S_2 \equiv S_4$ avec $\{\langle g, s\rangle, \langle g, x\rangle, \langle h, v\rangle, \langle h, y\rangle, \langle i, w\rangle, \langle i, t\rangle, \langle k, u\rangle, \langle k, z\rangle\}$.
- S_1, S_3 d'un côté et S_2, S_4 de l'autre sont distingués par la formule CTL $\mathbf{EX}\,\mathbf{EX}\,\alpha$.
- S_1 et S_3 sont distingués par $\mathbf{EX}\,\mathbf{AX}\,\beta$.

(b) Pour toute paire de structures S_i, S_j qui ne sont pas bisimilaires, dire si S_i simule S_j et/ou si S_j simule S_i (exhiber une relation de simulation si c'est le cas).

Solution :

- La formule LTL $(\mathbf{X}\,\mathbf{X}\,\beta) \rightarrow (\mathbf{G}\,\neg\gamma)$ est satisfaite par S_2 et S_4 mais pas par S_1 et S_3. Du coup, $S_1, S_3 \not\leq S_2, S_4$.
- $\mathbf{X}\,\mathbf{G}\,\neg\alpha$ convient pour prouver que $S_2, S_4 \not\leq S_1, S_3$.
- $S_1 \leq S_3$ avec $\{\langle a, m\rangle, \langle b, o\rangle, \langle b, p\rangle, \langle c, n\rangle, \langle d, o\rangle, \langle d, p\rangle, \langle e, q\rangle, \langle e, r\rangle, \langle f, q\rangle, \langle f, r\rangle\}$.
- $S_3 \leq S_1$ avec $\{\langle m, n\rangle, \langle n, c\rangle, \langle o, d\rangle, \langle p, d\rangle, \langle q, e\rangle, \langle q, f\rangle, \langle r, e\rangle, \langle r, f\rangle\}$.