Examen – Concepts et Model-Checking

18 mars 2024

1 LTL et Automates de Büchi

Soit $AP = \{p, q\}$, et soient ϕ, ψ les formules de LTL suivantes :

$$\phi = (\mathbf{F}\,\mathbf{G}\,p) \to (\mathbf{F}\,\mathbf{G}\,q) \qquad \text{et} \qquad \psi = (\mathbf{F}\,p) \land (\mathbf{G}\,q)$$

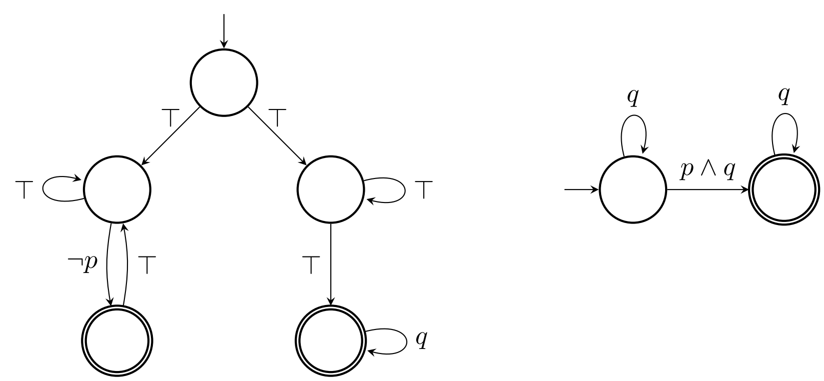
(a) Donner des automates de Büchi pour ϕ et pour ψ.
(Un automate ad-hoc suffit. L'utilisation de la construction systématique montrée en cours n'est ni exigée ni recommandée.)

(b) Est-ce que ϕ implique ψ ? Si ce n'est pas le cas, donner un mot infini sur 2^{AP} qui satisfait ϕ mais pas ψ.

(c) La même question que (b) avec les rôles de ϕ et ψ inversés.

Solution :

(a) Pour ϕ, avec une simple transformation, on obtient $\phi \equiv (\mathbf{G}\,\mathbf{F}\,\neg p) \lor (\mathbf{F}\,\mathbf{G}\,q)$, on construit donc la juxtaposition de deux automates simples.

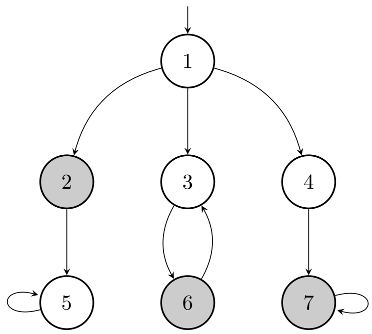


(b) ϕ n'implique pas ψ car $\emptyset^\omega$ est modèle de ϕ mais pas de ψ.

(c) Par contre, ψ implique ϕ: si q est toujours vrai, $\mathbf{F}\,\mathbf{G}\,q$ tient aussi.

2 CTL

On considère la structure $\mathcal{K}$ suivante, avec le seul prédicat p. Les états qui satisfont p sont indiqués en gris.



(a) Pour les formules suivantes, donner les états de $\mathcal{K}$ qui satisfont la formule.

- $\mathbf{AF}\, p$;
- $\mathbf{EG}\, p$;
- $\mathbf{AG}\,\mathbf{AF}\, p$;
- $\mathbf{AF}\,\mathbf{EG}\, p$;

(b) Trouver un état de $\mathcal{K}$ qui satisfait $\mathbf{EG}\,\mathbf{AF}\, p$ mais pas $\mathbf{AG}\,\mathbf{AF}\, p$ (s'il existe).

(c) Trouver un état de $\mathcal{K}$ qui satisfait $\mathbf{EF}\,\mathbf{EG}\, p$ mais pas $\mathbf{AF}\,\mathbf{EG}\, p$ (s'il existe).

Solution :

(a)
- $[\![\mathbf{AF}\, p]\!] = \{1, 2, 3, 4, 6, 7\}$;
- $[\![\mathbf{EG}\, p]\!] = \{7\}$;
- $[\![\mathbf{AG}\,\mathbf{AF}\, p]\!] = \{3, 4, 6, 7\}$;
- $[\![\mathbf{AF}\,\mathbf{EG}\, p]\!] = \{4, 7\}$.

(b) L'état 1 convient.

(c) Pareil.

3 CTL vs LTL

Étant donné une formule LTL ϕ et une formule CTL ψ, on considère ϕ et ψ équivalentes si, pour toute structure de Kripke $\mathcal{K}$ avec état initial r, on a $\mathcal{K} \models \phi \Leftrightarrow r \in [\![\psi]\!]_{\mathcal{K}}$.

Pour $n \geq 1$ on considère la formule LTL $\phi_n := \mathbf{X}^n p \vee \mathbf{F}\, q$.

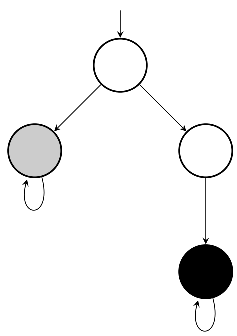
(a) Montrer que ϕ_1 n'est pas équivalent à $\psi := \mathbf{AX}\, p \vee \mathbf{AF}\, q$, i.e. trouver une structure telle que tout chemin est modèle de ϕ_1 mais l'état initial ne satisfait pas ψ.

(b) Trouver une formule CTL ψ_1 équivalente à ϕ_1.

(c) Généralement, pour $n > 1$, trouver une formule CTL ψ_n équivalente à ϕ_n.

Solution :

(a) Dans la structure ci-dessous, l'état gris satisfait p et l'état noir satisfait q. On a bien que tout chemin depuis l'état initial est modèle de soit $\mathbf{X}\, p$ ou de $\mathbf{F}\, q$. Mais ψ exige que soit tout chemin fait l'un, soit tout chemin fait l'autre, ce qui n'est pas le cas.



(b) $\psi_1 = q \vee \mathbf{AX}\,(p \vee \mathbf{AF}\, q)$.

(c) Tout chemin doit soit comporter un état avec p après n étapes ou un état q n'importe où. Dans les branches qui contiennent q avant n étapes on peut arrêter à vérifier. Du coup, avec ψ_1 de la partie (b), on définit, pour tout $n > 1$:

$$\psi_n = q \vee \mathbf{AX}\, \psi_{n-1}$$

4 Diagrammes de décision binaires

(a) Soient x_1, x_2, x_3, x_4 des variables binaires. La fonction de *parité* f_p est celle qui donne 1 si $x_1 + x_2 + x_3 + x_4$ est pair. La fonction f_1 vaut $(x_1 \wedge x_2 \wedge x_3) \vee (\neg x_2 \wedge x_4)$.

Pour l'ordre $x_1 \prec x_2 \prec x_3 \prec x_4$, donner des BDD pour f_p et f_1.

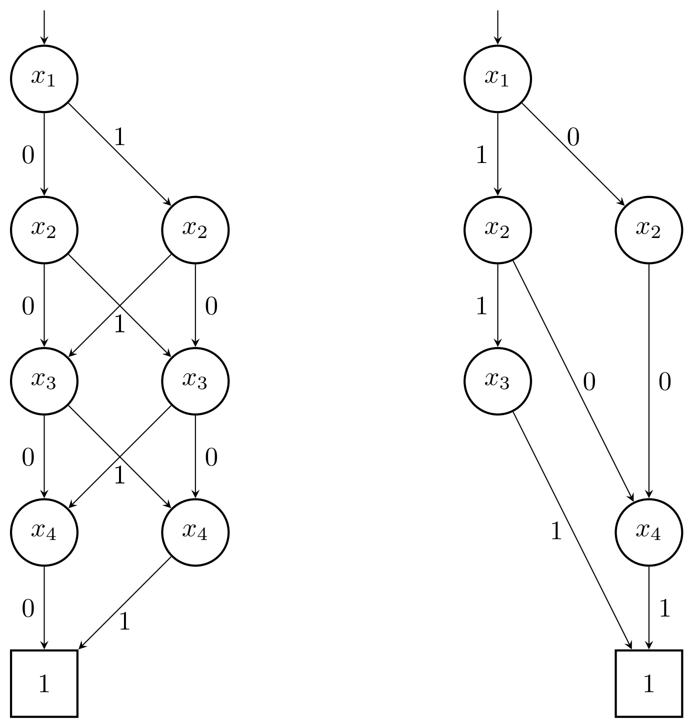
(b) Dans le suivant, on va dire qu'un BDD est de taille n s'il possède n sommets étiquetés par des variables (donc en excluant les feuilles 0 et 1).

Soient x, y deux variables avec $x \prec y$. Combien de BDD distincts existe-il

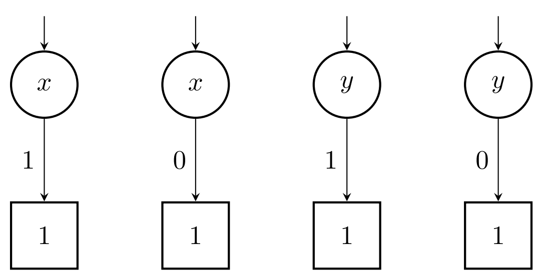
(i) de taille 1 ?
(ii) de taille 2 ?
(iii) de taille 3 ?

Solution :

(a) Pour f_p, les sommets dans la colonne gauche représentent le cas où la somme est paire, ceux dans la colonne droite le cas impair.

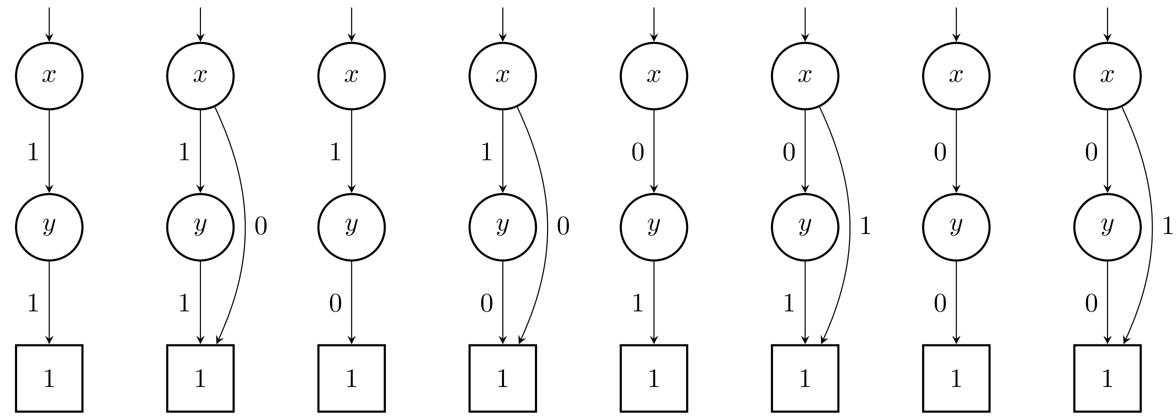


(b.i) Le seul sommet est étiqueté par x ou y; afin qu'il ne soit pas redondant, une seule arête mène à la feuille 1. Il y a donc 4 possibilités :

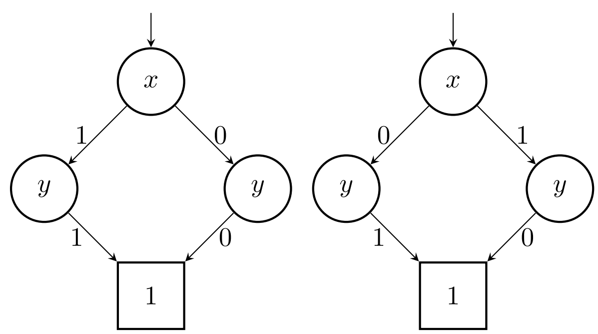


(b.ii) Pour avoir deux sommets, la racine porte forcement un x et le second sommet un y. Il nous reste trois choix indépendants:

- Pour le sommet y, il y a deux types (“y vrai” ou “y faux”).
- L'arête allant de x vers y porte 0 ou 1.
- L'autre arête sortante de x mène à 0 ou 1.



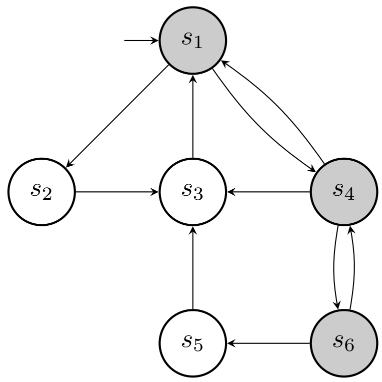
(b.iii) Pour avoir trois sommets, il faut une racine avec x et deux sommets avec y, tous les deux accessibles depuis la racine.



Notons que nous avons trouvé $4 + 8 + 2 = 14$ parmi les $2^{(2^2)} = 16$ fonctions binaires sur deux variables. Les deux restantes sont “constant 0” et “constant 1” dans lesquelles x et y sont tous les deux redondants.

5 Bisimulation

Dans la structure $\mathcal{K}$ ci-dessous, il y a un seul prédicat p, les états satisfaisant p sont indiqués en gris.



(a) Pour toute paire d'états, existe-il une formule de CTL qui est vrai pour l'un mais non pour l'autre ? (Le cas échéant, il suffit de dire «tel état est le seul à satisfaire telle formule» ou similaire.)

(b) En conclure en donnant la plus petite structure (en nombre d'états) bisimilaire à $\mathcal{K}$.

Solution :

(a) L'état s_3 est le seul à satisfaire $\mathbf{AX}\, p$.
Les états s_2 et s_5 sont les seuls à satisfaire $\mathbf{AX}\, \neg p$.
Les états s_1 et s_6 sont les seuls à satisfaire $\mathbf{EX}\, \mathbf{AX}\, \neg p$.
Du coup, l'état s_4 est le seul à satisfaire la négation de ces trois formules.
Les états s_2 et s_5 ne sont distingués par aucune formule : ils sont $\neg p$ et mènent à s_3.
Les états s_1 et s_6 ne sont distingués par aucune formule : ils sont p et mènent soit à s_4, soit à s_2 resp. s_5 qui sont eux indistinguables.

(b) On fusionne les paires d'états non distinguables, avec la relation de bisimulation naturelle : $\{\langle s_1, t_{16}\rangle, \langle s_2, t_{25}\rangle, \langle s_3, t_3\rangle, \langle s_4, t_4\rangle, \langle s_5, t_{25}\rangle, \langle s_6, t_{16}\rangle\}$