Vendredi 24 octobre 2008
Durée : 4 heures
Documents autorisés

Examen : Programmation et Logique
Master 2 Recherche 2008-2009

Attention : donnez autant de détails que vous jugez nécessaire ; des simples copies-collers-miroirs de vos notes de cours ne seront pas jugés satisfaisants. En bref, montrez que vous avez compris.
Attention : la méthode d'évaluation indiqué (c-à-d. les pts.) est provisoire et susceptible d'être modifiée.

Le théorème de complétude

En discutant le théorème de complétude pour la logique du premier ordre, nous avons procédé comme suit. Étant donné un séquent $\Gamma \vdash \Delta$ qui n'est pas prouvable dans le système des séquents LK, nous avons construit une suite de séquents $\Gamma_n \vdash \Delta_n$ avec certaines propriétés.
De cette suite, nous avons construit un modèle $\mathcal{M}$ et une valuation $\nu : X \to \mathcal{M}$. Nous avons prouvé le Lemme suivant :

Lemme 0.1. *Pour toute formule ϕ, si $\phi \in \bigcup_{n\geq 0} \Gamma_n$ alors $\mathcal{M}, \nu \models \phi$, et si $\phi \in \bigcup_{n\geq 0} \Delta_n$, alors $\mathcal{M}, \nu \not\models \phi$.*

Nous avons exposé les détails de la preuve par induction pour les cas où ϕ est une formule de la forme $A \vee B$ ou bien de la forme $\forall z.A[z]$.

Exercice 1. (2 points). Exposez les détails de la preuve par induction du Lemme pour le cas d'une formule ϕ de la forme $A \wedge B$.

Solution. Soit donc $\phi = A \wedge B$, et supposonns (hypothèse d'induction) que le Lemme est vrai pour A, B.
Si $A \wedge B \in \bigcup_{n\geq 0} \Gamma_n$ – disons $A \wedge B \in \Gamma_n$ – alors pour $n' \geq n$, $A \wedge B$ est en tête de la liste $\omega_{n'}$ et par construction $A, B \in \Gamma_{n'+1}$. Par hypothèse d'induction, $\mathcal{M}, \nu \models A$, $\mathcal{M}, \nu \models B$, et donc $\mathcal{M}, \nu \models A \wedge B$.
Si $A \wedge B \in \bigcup_{n\geq 0} \Delta_n$ – disons $A \wedge B \in \Delta_n$ – alors pour $n' \geq n$, $A \wedge B$ est en tête de la liste $\omega_{n'}$ et par construction ou bien $A \in \Delta_{n'+1}$, ou bien $B \in \Delta_{n'+1}$. Supposons maintenant que $A \in \Delta_{n'+1}$, il decoule de l'hypothèse d'induction que $\mathcal{M}, \nu \not\models A$ et, par conséquent, $\mathcal{M}, \nu \not\models A \wedge B$. De façon semblable, si $B \in \Delta_{n'+1}$, on démontre que $\mathcal{M}, \nu \not\models A \wedge B$. $\square$

Décidabilité

Exercice 2. (3 points). Soit $\mathcal{L} = \langle X, F, P, ar \rangle$ un langage tel que F est un ensemble fini de symboles de fonctions, tel que $ar(f) = 0$ pour tout $f \in F$. Soit $\mathcal{F}_{\mathcal{L}\forall}$ l'ensemble des formules universelles de ce langage, c-à-d. $\phi \in \mathcal{F}_{\mathcal{L}\forall}$ si ϕ est de la forme

$$\phi = \forall x_1 \ldots \forall x_n.\psi$$

où ψ ne contient pas des quantificateurs. Montrez que le problème $\langle I, P \rangle$, où $I = \mathcal{F}_{\mathcal{L}\forall}$ et $P(\phi) = Oui$ si et seulement si ϕ possède un modèle, est décidadable.
Suggestion :

(i). Montrez que, pour $\phi \in \mathcal{F}_{\mathcal{L}\forall}$, si $\mathcal{M} \models \phi$ et $\mathcal{M}'$ est un sous-modèle de $\mathcal{M}$, alors $\mathcal{M}' \models \phi$.

(ii). Montrez que si $\phi \in \mathcal{F}_{\mathcal{L}\forall}$ a un modèle, alors ϕ a un modèle fini.

(iii). Tirez la conclusion.

Solution. (i) Rappelons d'abord que signifie que $\mathcal{N}$ est un sous modèle de $\mathcal{M}$ (par rapport a ce langage $\mathcal{L}$).
Soit donc $\mathcal{M} = \langle M, I \rangle$ (M un esemble et I une interpretation du langage $\mathcal{L}$). On dit que $\mathcal{N} = \langle N, I' \rangle$ est un sous modèle de $\mathcal{M}$ si $N \subseteq M$, $I(c) = I'(c) \in N$ pour toute constante $c \in F$, et $(m_1, \ldots, m_n) \in I'(R)$ si et seulement si $(m_1, \ldots, m_n) \in I(R)$ pour tout tuplet $(m_1, \ldots, m_n) \in N^n$.
Remarquons aussi qu'étant donné $N \subseteq M$ tel que $I(c) \in N$ pour toute consrante $c \in F$, on a qu'il existe une seule interpretantion I' tel que $\mathcal{N} = \langle N, I' \rangle$ est un sous modèle de $\mathcal{M}$.

Montrons maintenant que si $\phi = \forall x_1, \ldots, x_n.\psi \in \mathcal{F}_{\mathcal{L}\forall}$, $\mathcal{M} \models \phi$ et $\mathcal{N}$ est un sous-modèle de $\mathcal{N}$, alors $\phi \models \mathcal{N}$.
Or pour montrer que $\mathcal{N} \models \phi$, il faut montrer que $\mathcal{N}, \nu \models \psi$, où $nu : X \longrightarrow N \subseteq M$ est une valuation arbitraire.

Car ψ est une formule propositionnelle, un simple induction à partir des formules atomiques montrera que $\mathcal{N}, \nu \models \psi$ si et seulement $\mathcal{M}, \nu \models \psi$. Or la dernière condition est vraie car $\mathcal{M} \models \phi$ implique que $\mathcal{M}, \nu \models \psi$ pour toute valuation ν des variables individuelles. Récapitulons : $\mathcal{M} \models \phi$ implique $\mathcal{M}, \nu \models \psi$, ce que implique $\mathcal{N}, \nu \models \psi$.

(ii) Soit $\mathcal{M} \models \phi$, avec $\mathcal{M} = \langle M, I \rangle$. Or soit $N \subseteq M$ définit par

$$N = \{ I(c) \mid c \in F \} .$$

Car F est fini, on a que N est fini, et observons aussi que $\mathrm{card}\, N \leq \mathrm{card}\, F$. Si $\mathcal{N}$ est le seul sous-modèle de $\mathcal{M}$ tel que $\mathcal{N} = \langle N, I' \rangle$ alors, à cause de (i) on a que $\mathcal{N} \models \phi$: $\mathcal{N}$ est donc un modèle fini de ϕ.

(iii) La discussion précedente montre que $\phi \in \mathcal{F}_{\mathcal{L}\forall}$ possède un modèle si et seulement si il possède un modèle de taille au plus $\mathrm{card}\, F$.
Un algorithme (où machine de Turing) pour décider le problème $\langle \mathcal{F}_{\mathcal{L}\forall}, P \rangle$ construira l'un après l'autre tous le modèles $\mathcal{M}$ du langage $\mathcal{L}$ de taille au plus $\mathrm{card}\, F$ en vérifiant si $\mathcal{M} \models \phi$ – si c'est le cas il répondra *Oui*, sinon il passera au modèle suivant. Si après avoir construit tous ces modèles il n'a pas trouvé un modèle $\mathcal{M}$ tel que $\mathcal{M} \models \phi$, alors l'algorithme répondra *Non*. □

Logique dynamique propositionnelle

Exercice 3. (2 points). Rappelons la règle du conditionnel de la logique de Hoare :

$$\frac{\{ \psi_1 \land \phi \} \alpha \{ \psi_2 \} \qquad \{ \psi_1 \land \neg\phi \} \beta \{ \psi_2 \}}{\{ \psi_1 \} \texttt{if } \phi \texttt{ then } \alpha \texttt{ else } \beta \{ \psi_2 \}}$$

(i). Rappelez comment on peut coder une assertion de la forme $\{ \phi \} \alpha \{ \psi \}$ par une formule $\ulcorner \{ \phi \} \alpha \{ \psi \} \urcorner^{\mathcal{F}}$ de PDL.

(ii). Rappelez comment on peut coder un programme de la forme $\texttt{if } \phi \texttt{ then } \alpha \texttt{ else } \beta$ par un programme de PDL $\ulcorner \texttt{if } \phi \texttt{ then } \alpha \texttt{ else } \beta \urcorner^{\mathcal{P}}$.

(iii). Montrez que la règle ci-dessus est correcte : si $\ulcorner \{ \psi_1 \land \phi \} \alpha \{ \psi_2 \} \urcorner^{\mathcal{F}}$ et $\ulcorner \{ \psi_1 \land \neg\phi \} \beta \{ \psi_2 \} \urcorner^{\mathcal{F}}$ sont des tautologies de PDL, alors $\ulcorner \{ \psi_1 \} \texttt{if } \phi \texttt{ then } \alpha \texttt{ else } \beta \{ \psi_2 \} \urcorner^{\mathcal{F}}$ est aussi une tautologie de PDL.

Solution. (i) Posons

$$\ulcorner \{ \phi \} \alpha \{ \psi \} \urcorner^{\mathcal{F}} = \phi \to [\alpha]\psi .$$

(ii) Posons

$$\ulcorner \texttt{if } \phi \texttt{ then } \alpha \texttt{ else } \beta \urcorner^{\mathcal{P}} = (?\phi \cdot \alpha) \cup (?\neg\phi \cdot \alpha) .$$

(iii) Rappelons d'abord que $\phi \to [\alpha]\psi$ est une tautologie de PDL ssi poir n'importe quel modèle $\mathcal{M}$, on a

$$\phi^{\mathcal{M}} \subseteq [\alpha]\psi^{\mathcal{M}}$$

où

$$\phi^{\mathcal{M}} = \{ s \in M \mid s \models \phi \} .$$

Soit donc $\mathcal{M}$ arbitraire – on écrira pas ensuite les super-scripts $\mathcal{M}$ dans $\phi^{\mathcal{M}}$. On a que $\psi_1 \cap \phi \subseteq [\alpha]\psi_2$, ce qui est équivalent à

$$\begin{aligned} \psi_1 &\subseteq \phi \to [\alpha]\psi_2 \\ &= [?\phi][\alpha]\psi_2 \\ &= [?\phi \cdot \alpha]\psi_2 . \end{aligned}$$

De façon semblable, $\psi_1 \cap \neg\phi \subseteq [\beta]\psi_2$ est équivalent à

$$\psi_1 \subseteq [?\neg\phi \cdot \beta]\psi_2\,,$$

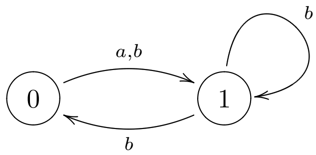
d'où

$$\begin{aligned}\psi_1 &\subseteq [?\phi \cdot \alpha]\psi_2 \cap [?\neg\phi \cdot \beta]\psi_2 \\ &= [?\phi \cdot \alpha \cup ?\neg\phi \cdot \beta]\psi_2\,.\end{aligned}$$

$\square$

Le μ-calcul

Exercice 4. (3 points). Soient ϕ la formule $\nu_x.\langle a\rangle(x \vee \mu_y.(\langle b\rangle x \wedge [a]y))$ du μ-calcul et $\mathcal{M}$ le système de transition suivant :

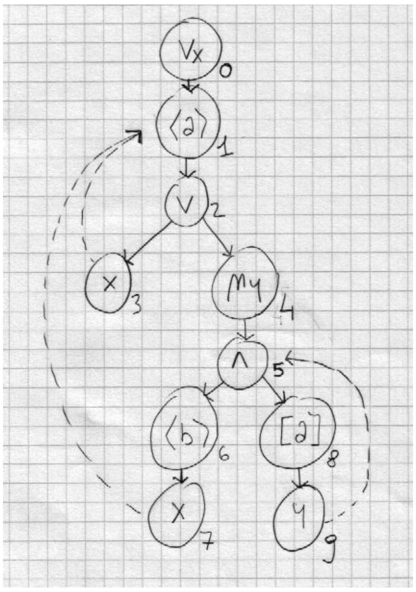


(i). Construisez le jeu $\mathcal{G}(\mathcal{M}, \phi)$: dessinez le graphe des positions et des mouvements, étiquétez les positions par un joueur.

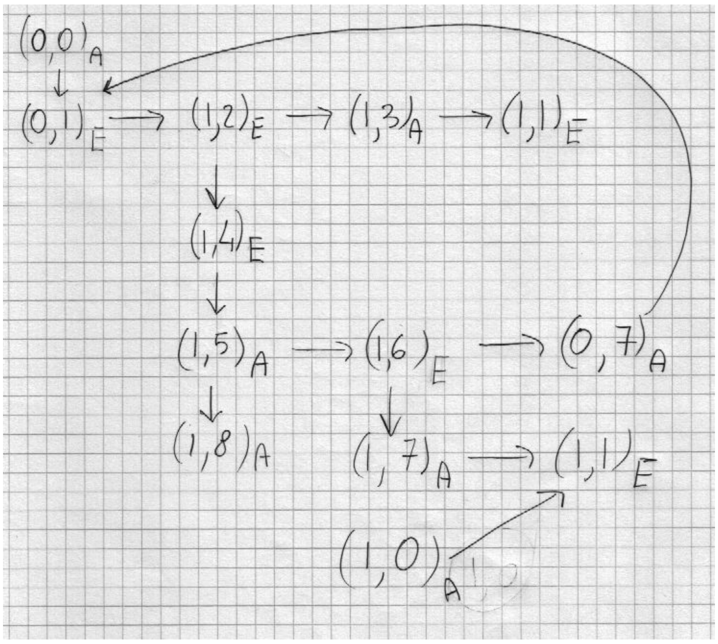
(ii). Explicitez dans ce jeu la condition de gagne pour les parties infinies.

(iii). Est ce que $\mathcal{M}, 0 \models \phi$? Est ce que $\mathcal{M}, 1 \models \phi$? Justifiez vos réponses.

Solution. (i) Dessinons d'abord l'arbre avec retours de la formule ϕ en numerotant les sommets :



Le jeu $\mathcal{G}(\mathcal{M}, \phi)$ est alors comme suit :



Remarque : dans le dessins ci-dessus la position $(1,1)$ a été dessiné deux fois.

(ii) Rappelons que Eva gagne une partie infinie d'un jeu de la forme $\mathcal{G}(\mathcal{M},\phi)$ ssi la variable sur ce chemin visitée infiniment souvent dont le retour est plus proche de la racine, est une variable de type ν. En particulier, dans le jeu ci-dessus, la seule partie infinie possible est de la forme

$$(0,0)((0,1)(1,2)(1,4)(1,5)(1,5)(0,7))^{\omega}$$

et la variable visitée infiniment souvent dont le retour est plus proche de la racine est 7, i.e. la variable x, qui étant liée par ν, est une variable de type ν. Il s'agit donc d'une partie infinie gagnée par Eva.

(iii) On remarque que Eva a une stratégie qui oblige Adam à parcourir la seule partie infinie, ou bien d'atteindre la position $(1,8)$ qui est perdante pour Adam. Il s'agit donc d'une stratégie gagnante pour Eva à partir de la position $(0,0)$. Par conséquent

$$\mathcal{M}, 0 \models \phi\,.$$

Par contre, de la position $(1,0)$ Adam peut forcer Eva dans la position $(1,1)$, perdante pour Eva. Il s'agit donc d'une stratégie gagnante pour Adam à partir de la position $(1,0)$ et par conséquent

$$\mathcal{M}, 1 \not\models \phi\,.$$

□

Exercice 5. (3 points). Considérez la formule du μ-calcul

$$\mathcal{U}(x,y) = \mu_z.(y \vee (x \wedge \langle a \rangle z))\,.$$

Considérons le système de transition $\mathcal{N} = \langle \mathbb{N}, \xrightarrow{a} \rangle$, où $\mathbb{N}$ est l'ensemble des entiers positifs et $n \xrightarrow{a} m$ si et seulement si $m = n+1$. Montrez que (étant donné une valuation arbitraire $v : X \longrightarrow \mathcal{P}(\mathbb{N})$) on a

$$n \models \mathcal{U}(x,y) \;\text{ ssi }\; \exists k \geq 0 \;\text{ t.q. }\; n+k \models y \text{ et}, \text{ pour tout } i = 0,\ldots,k-1,\; n+i \models x\,.$$

Solution. Regardons la structure du jeu $\mathcal{G}(\mathbb{N},\mathcal{U}(x,y))$ de la position $(n+i, y \vee (\ldots))$:

$$\begin{tikzcd}
(n+i,\vee)_E \arrow[r] \arrow[d] & (n+i,\wedge)_A \arrow[r] \arrow[d] & (n+i,\langle a\rangle)_E \arrow[r] & (n+i+1,z)_E \arrow[r] & (n+i+1,\vee)_E \arrow[r] \arrow[d] & \cdots \\
(n+i,y) & (n+i,x) & & & (n+i+1,y) &
\end{tikzcd}$$

S'il existe $k \geq 0$ t.q. $n+k \models y$ et $n+i \models x$ pour tout $i = 0, \ldots, k-1$, alors Eva peut utiliser la strategie suivante de $(n, \vee)$ – et donc de $(n, \mathcal{U}(x,y))$ – dans le jeu. Eva choisira des mouvements en horizontal pour se rendre de $(n, \vee)$ à $(n+k, \vee)$ et puis à $(n+k, y)$. Cette dernière est une position gagnante pour Eva car $n+k \models y$ (et donc $n+k \in v(y)$, $(n+k, y)$ est une position d'Adam ou il ne peut pas jouer). Si, pendant ce chemin en horizontal, Adam choisit le mouvement $(n+i, \wedge) \rightarrow (n+i, x)$, alors Adam il perdra de cette position, car $n+i \models x$.
Supposons par contre que $n \models \mathcal{U}(x,y)$, c-à-d. que Eva possède une stratégie gagnante de $(n, \mathcal{U}(x,y))$ et donc de $(n, \vee)$. Cette stratégie lui suggérera de choisir un chemin en horizontal, pour aboutir à la position $(n+k, \vee)$ et puis à $(n+k, y)$ – un chemin en horizontal infini n'est pas possible car il serait perdant pour Eva. Car $(n+k, y)$ est gagnant pour Eva, alors $n+k \models y$. Dans ce chemin en horizontal, pour $i = 0, \ldots, k-1$, Adam pourrait bien choisir le mouvement $(n+i, \wedge) \rightarrow (n+i, x)$, mais car cette position est gagnante pour Eva, on a $n+i \models x$. $\square$

Automates sur les mots infinis

Exercice 6. (2 points). Soit $\mathcal{A}_2 = \langle Q, q_0, \{ \xrightarrow{a} \}_{a \in \Sigma_2}, F \rangle$ un automate de Buchi et soit $f : \Sigma_1 \longrightarrow \Sigma_2$ une fonction de ré-étiquetage de l'alphabet Σ_1 dans l'alphabet Σ_2.

(i). Proposez un automate $\mathcal{A}_1$ tel que $\mathcal{L}(\mathcal{A}_1) = \{ \sigma \in \Sigma_1^\omega \mid f \circ \sigma \in \mathcal{L}(\mathcal{A}_2) \}$ – décrivez formellement cet automate.

(ii). Démontrez l'égalité

$$\mathcal{L}(\mathcal{A}_1) = \{ \sigma \in \Sigma_1^\omega \mid f \circ \sigma \in \mathcal{L}(\mathcal{A}_2) \} .$$

Solution. (i) Définissons $\mathcal{A}_1 = \langle Q, q_0, \{ \xrightarrow{b} \}_{b \in \Sigma_1}, F \rangle$ avec

$$q \xrightarrow{b} q' \text{ ssi } q \xrightarrow{f(b)} q' .$$

(ii) Soit $\beta \in \mathcal{L}(\mathcal{A}_1)$ et $\rho = q_0 \xrightarrow{b_1} q_1 \xrightarrow{b_2} q_2 \ldots$ un run dans l'automate $\mathcal{A}_1$ qui accepte le mot $\beta = b_1 b_2 \ldots$. Alors, cette même suite est un run $\rho = q_0 \xrightarrow{f(b_1)} q_1 \xrightarrow{f(b_2)} q_2 \ldots$ de $f \circ \sigma$ dans l'automate $\mathcal{A}_2$. On a donc que

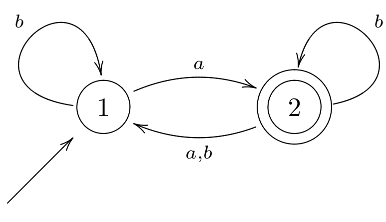
$$\mathcal{L}(\mathcal{A}_1) \subseteq \{ \beta \mid f \circ \beta \in \mathcal{L}(\mathcal{A}_2) \} .$$

Soit maintenant β tel que $f \circ \beta \in \mathcal{L}(\mathcal{A}_2)$. Soit donc $\rho = q_0 \xrightarrow{f(b_1)} q_1 \xrightarrow{f(b_2)} q_2 \ldots$ un run de l'automate $\mathcal{A}_2$ qui accepte $f \circ \beta$. Évidemment, cette même suite est un run $\rho = q_0 \xrightarrow{b_1} q_1 \xrightarrow{b_2} q_2 \ldots$ de l'automate $\mathcal{A}_2$ qui accepte β. On a donc

$$\{ \beta \mid f \circ \beta \in \mathcal{L}(\mathcal{A}_2) \} \subseteq \mathcal{L}(\mathcal{A}_1) .$$

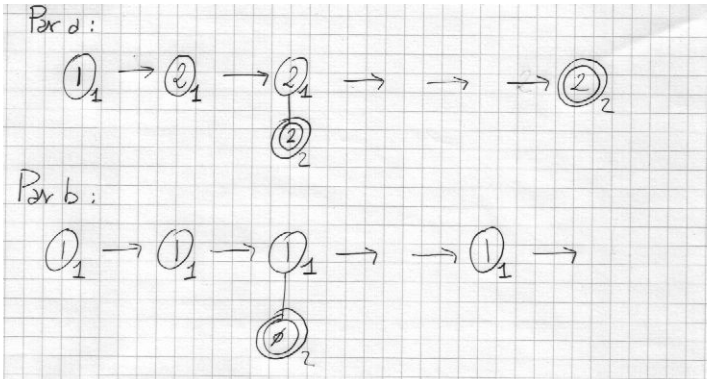
$\square$

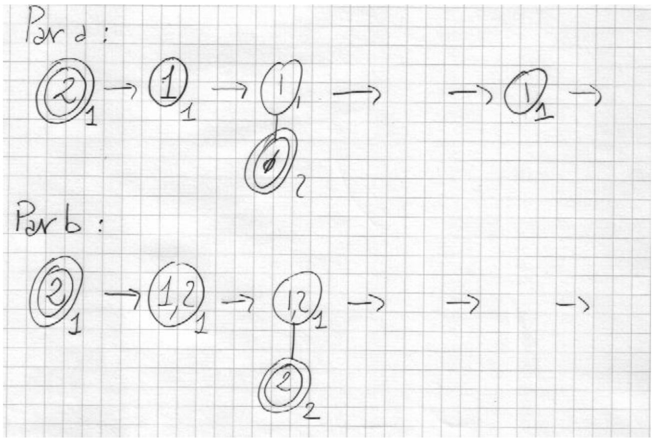
Exercice 7. (3 points). Considérez l'automate de Buchi suivant :

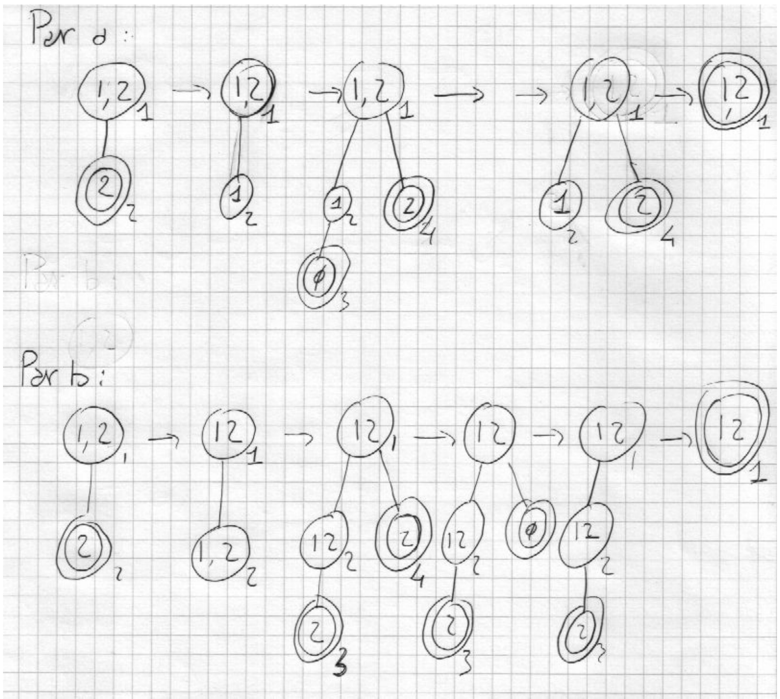


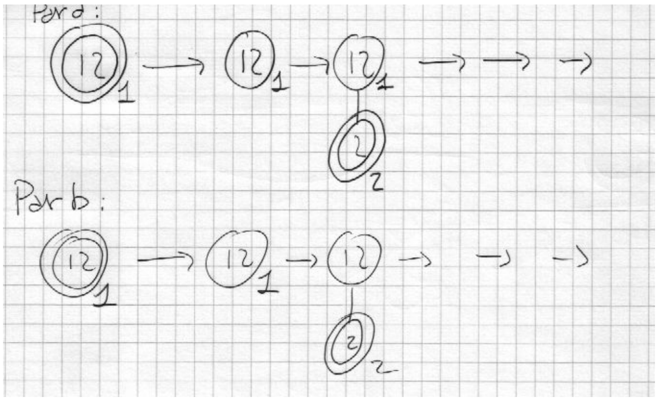
En utilisant la procédure de détermination de Safra, construisez un automate de Rabin déterministe équivalent à cet automate. Documentez, étape par étape, cette procedure.

Solution. Nous développons cet exercice comme d'habitude.

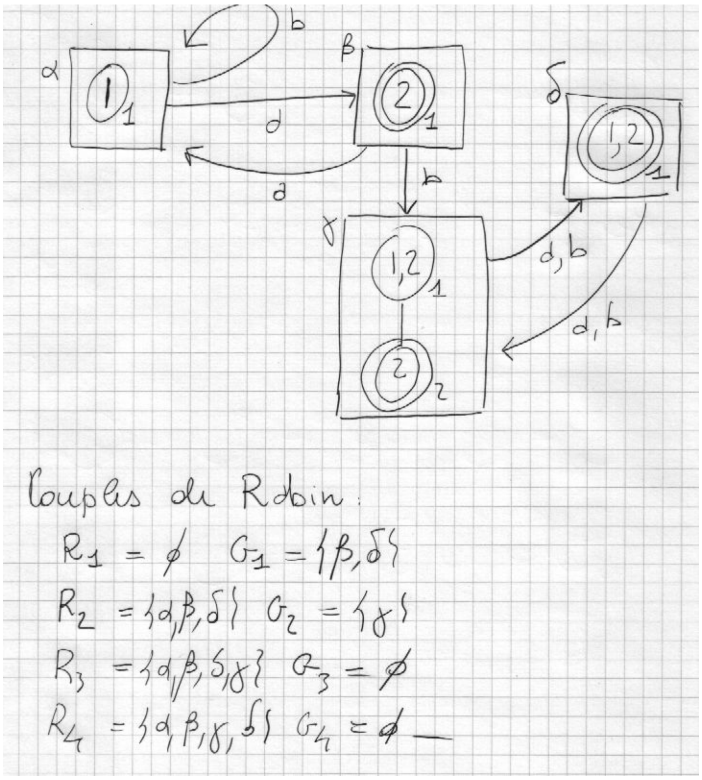

Par d :
Par b :


Par d :
Par b :


Par d :
Par b :



L'automate (avec la condition d'acceptance explicitée) est donc :



□

Logique monadique du second ordre

Exercice 8. (3 points).

(i). Rappelez la syntaxe de la logique monadique du second ordre (MSOL) ainsi que celle de la logique monadique du second ordre *pure* (MSOP).

(ii). Montrez que pour toute formule $\phi \in \mathcal{F}_{MSOL}$ il existe une formule $\phi' \in \mathcal{F}_{MSOP}$ telle que, si $Free(\phi) = \{ x_1, \ldots, x_n, X_1, \ldots, X_m \}$, alors $Free(\phi') = \{ Y_1, \ldots, Y_n, X_1, \ldots, X_m \}$ et ϕ' satifait la relation

$$v, w \models \phi \quad \text{ssi} \quad w' \models \phi' ,$$

où w' est une valuation des variables propositionnelles (ou monadique) satisfaisant

$$w'(Y_i) = \{ v(x_i) \} , \ \ i = 1, \ldots, n , \qquad\qquad w'(X_j) = w(X_j) , \ \ j = 1, \ldots, m .$$

Solution. (i) L'ensemble $\mathcal{F}_{MSOL}$ (des formules de la logique monadique du second ordre) est défini la grammaire suivante :

$$\begin{aligned}\phi = \ & 0(x) \mid xSy \mid \phi \wedge \phi \mid \neg\phi \mid \exists x.\phi \\ & \mid \emptyset \mid \mathbf{0} \mid x \in X \mid X \subseteq Y \mid X \mid X\mathbf{S}Y \mid \exists X.\phi\,.\end{aligned}$$

Par contre, l'ensemble $\mathcal{F}_{MSOP}$ (des formules de la logique monadique du second ordre *pure*) est défini par la grammaire suivante :

$$\begin{aligned}\phi = \ & \phi \wedge \phi \mid \neg\phi \mid \\ & \mid \emptyset \mid \mathbf{0} \mid X \subseteq Y \mid X \mid X\mathbf{S}Y \mid \exists X.\phi\,.\end{aligned}$$

Nous observons d'abord que la propriété « être in singleton » est definissable dans la logique monadique du second ordre *pure*. Posons :

$$\mathit{Singl}(X) = \neg(X \subseteq \emptyset) \wedge \forall Y.(Y \subseteq X \implies Y \subseteq \emptyset \vee X \subseteq Y)\,.$$

Remarque : ici $\forall$, $\implies$, $\vee$, sont definissables comme d'habitude, par exemple $\forall Y.\Phi = \neg\exists Y.\neg\Phi$.
En suite, nous definissons $\phi' = \lceil\phi\rceil \in \mathcal{F}_{MSOP}$, par induction sur la structure de $\phi \in \mathcal{F}_{MSOL}$, comme suit :

$$\begin{aligned}
\lceil 0(x) \rceil &= \mathit{Singl}(X) \wedge X \subseteq \mathbf{0} \\
\lceil xSy \rceil &= \mathit{Singl}(X) \wedge \mathit{Singl}(Y) \wedge X\mathbf{S}Y \\
\lceil \phi \wedge \phi \rceil &= \lceil\phi\rceil \wedge \lceil\phi\rceil \\
\lceil \neg\phi \rceil &= \neg\lceil\phi\rceil \\
\lceil \exists x.\phi \rceil &= \exists X.(\mathit{Singl}(X) \wedge \lceil\phi\rceil) \\
\lceil \emptyset \rceil &= \emptyset \\
\lceil \mathbf{0} \rceil &= \mathbf{0} \\
\lceil x \in X \rceil &= \mathit{Singl}(X') \wedge X' \subseteq X \\
\lceil X \subseteq Y \rceil &= X \subseteq Y \\
\lceil X\mathbf{S}Y \rceil &= X\mathbf{S}Y \\
\lceil \exists X.\phi \rceil &= \exists X.\lceil\phi\rceil\,.
\end{aligned}$$

□