Lundi 2 novembre 2009 — Examen : Programmation et Logique
Durée : 4 heures — Master 2 Recherche 2009-2010
Documents autorisés

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 indiquée (c-à-d. les pts.) est provisoire et susceptible d'être modifiée.

Le calcul des séquents

Exercice 1. (2 points). Rappelons qu'un séquent $\Gamma \vdash \Delta$ est valide si $\mathcal{M}, v \models \bigwedge \Gamma \to \bigvee \Delta$ pour tout modèle $\mathcal{M}$ et toute valuation $v : X \longrightarrow |\mathcal{M}|$. Une régle de la forme

$$\frac{\Gamma \vdash \Delta}{\Gamma' \vdash \Delta'}$$

est correcte si $\Gamma' \vdash \Delta'$ est valide si $\Gamma \vdash \Delta$ est valide. Montrez que la régle d'introduction à droite du quantificateur universel

$$\frac{\Gamma \vdash A[x], \Delta}{\Gamma \vdash \forall x.A[x], \Delta} \; x \text{ n'est pas libre dans } \Gamma, \Delta$$

est correcte.

Solution. Soient $\mathcal{M}, v$ arbitraires. On veut montrer que

$$\mathcal{M}, v \models \bigwedge \Gamma \to \forall x.A[x] \vee \bigvee \Delta \,, \tag{1}$$

en sachant que $\mathcal{M}, v' \models \bigwedge \Gamma \to A[x] \vee \bigvee \Delta$ pour toute valuation v'.
La (1) est vraie si $\mathcal{M}, v \not\models \gamma$ pour une formule $\gamma \in \Gamma$, ou si $\mathcal{M}, v \models \delta$ pour une formule $\delta \in \Delta$.
Supposons donc que $\mathcal{M}, v \models \gamma$ pour tout $\gamma \in \Gamma$ et $\mathcal{M}, v \not\models \delta$ pour tout $\delta \in \Delta$. Sous ces conditions, la (1) est vraie si et seulement si $\mathcal{M}, v \models \forall x.A[x]$, ce qui revient à dire que $\mathcal{M}, v[m/x] \models A[x]$ pour tout $m \in \mathcal{M}$. Soit donc $m \in \mathcal{M}$ dorénavant fixé et montrons que $\mathcal{M}, v[m/x] \models A[x]$. Or nous avons que

$$\mathcal{M}, v[m/x] \models \bigwedge \Gamma \to A[x] \vee \bigvee \Delta \,, \tag{2}$$

D'ailleurs, x n'est pas une variable libre dans une formule $\phi \in \Gamma \cup \Delta$ et par conséquent, pour un tel ϕ, $\mathcal{M}, v[m/x] \models \phi$ si et seulement si $\mathcal{M}, v \models \phi$. Il en découle que $\mathcal{M}, v[m/x] \models \gamma$ pour tout $\gamma \in \Gamma$, $\mathcal{M}, v[m/x] \not\models \delta$ pour tout $\delta \in \Delta$, et la (2) implique alors $\mathcal{M}, v[m/x] \models A[x]$. □

Exercice 2. (3 points). En exposant le théorème de complétude pour la logique du premier ordre, nous avons construit, par induction, une suite $(\Gamma_n \vdash \Delta_n, \omega_n)$ avec certaines propriétés. Le details de la construction ont été exposés dans le cas que la première formule de ω_n soit une formule de la forme $A \vee B$ ou bien de la forme $\forall z.A[z]$.
- (2 points). Exposez les détails de cette construction, pour le cas où la tête de la liste ω_n est une formule de la forme $\neg A$.
- (1 points). (Montrez que s'il existe $n \geq 0$ tel que $\neg A \in \Gamma_n$, alors $\mathcal{M}, v \models \neg A$, et s'il existe $m \geq 0$ tel que $\neg A \in \Gamma_m$, alors $\mathcal{M}, v \not\models \neg A$).

Solution. Soit $(\Gamma_n \vdash \Delta_n, \omega_n)$ avec $\omega_n = \neg A, \Lambda$. Si $\neg A \in \Gamma_n$ alors nous posons

$$\Gamma_{n+1} = \Gamma_n \qquad\qquad \Delta_{n+1} = \Delta_n, A \,,$$

et si $\neg A \in \Delta_n$ alors nous posons

$$\Gamma_{n+1} = \Gamma_n, A \qquad\qquad \Delta_{n+1} = \Delta_n \,.$$

Dans tous les deux cas, nous posons

$$\omega_{n+1} = \Lambda, A, \neg A \,.$$

Supposons que $\neg A \in \Gamma_n$. Alors il existe $n' \geq n$ tel que $\neg A$ est en tête de $\omega_{n'}$ et, par conséquent, $A \in \Delta_{n'+1}$. Par hypothèse d'induction (sur A), $\mathcal{M}, v \not\models A$ et donc $\mathcal{M}, v \models \neg A$.
Supposons que $\neg A \in \Delta_m$. Alors il existe $m' \geq m$ tel que $\neg A$ est en tête de $\omega_{m'}$ et, par conséquent, $A \in \Gamma_{m'+1}$. Par hypothèse d'induction (sur A), $\mathcal{M}, v \models A$ et donc $\mathcal{M}, v \not\models \neg A$. □

Décidabilité

Exercice 3. (2 points). Esquissez un algorithme pour décider le problème (I, P) suivant :

$$I = \{ \phi \mid \phi \text{ est une formule de } \mathbb{PDL} \}$$

$$P(\phi) = \begin{cases} \texttt{Oui}, \text{ si } \phi \text{ est une tautologie de } \mathbb{PDL}, \text{ c-à-d. si } \mathcal{M}, v \models \phi, \text{ pour tout } \mathcal{M} \text{ et tout } v, \\ \texttt{Non}, \text{ sinon.} \end{cases}$$

Solution. Pour construire un algorithme T qui décide si une formule ϕ est une tautologie, nous allons utiliser un algorithme S qui décide si une formule ψ est satisfaisable, car ϕ est une tautologie ssi $\neg\phi$ n'est satisfaisable.
On aura donc

```
T φ
si S ¬φ alors
  retourner faux
else
  retourner vrai
```

En ce qui concerne l'algorithme S, nous allons nous servir du théorème du modèle fini, en sachant que si ψ a un modèle, alors il a un modèle de taille au plus $2^{|FL(\psi)|}$.

```
S ψ
pour tout modèle M = (S, { →^a }_{a∈act}) tel que |S| ≤ 2^{|FL(ψ)|}
     pour toute fonction v : FV(ψ) ⟶ P(S),
          pour tout s ∈ S,
               si M, v, s ⊨ ψ alors
                  retourner vrai
               fin si
          fin pour
     fin pour
fin pour
retourner faux
```

□

Logique modale, PDL, μ-calcul

Exercice 4. (4 points). Le but de cet exercice est de compléter la preuve de séparation entre $\mathbb{PDL}$ et $\mathbb{PDL}$ avec test. Vous allez démontrer certains faits qui ont été présenté sans preuve.
A ce fin, rappelons la définition (inductive) de l'ensemble d'entiers J_r dénoté par une expression régulière r sur l'alphabet $\Sigma = \{ a \}$:

$$\begin{aligned} J_a &= \{ 1 \}, \\ J_\emptyset &= \emptyset, & J_{r \cup r'} &= J_r \cup J_{r'}, \\ J_1 &= \{ 0 \}, & J_{r \cdot r'} &= \{ n + m \mid n \in J_r, m \in J_{r'} \}, \\ J_{r^*} &= \{ \sum_{i=1,\ldots,n} m_i \mid n \geq 0, m_i \in J_r \}. \end{aligned}$$

(i). (2 points). Prouvez le fait suivant : $\mathfrak{A}_m, v, k \models \langle r \rangle \psi$ *ssi il existe* $j \in J_r$ *tel que* $\mathfrak{A}_m, v, k + j \bmod 2m \models \psi$.

Solution. Soit $\widetilde{r} \subseteq \{ 0, \ldots, 2m-1 \} \times \{ 0, \ldots, 2m-1 \}$ l'interprétation usuelle d'une expression régulière comme une relation. Soit $[m] = \{ 0, \ldots, 2m-1 \}$, nous allons montrer l'égalité

$$\widetilde{r} = R(r) \tag{3}$$

où

$$\begin{aligned} R(r) &= \{ (k, k') \mid k, k' \in [m], \exists j \in J_r \text{ t.q. } k' = k + j \bmod 2m \}. \\ &= \{ (k, (k + j) \bmod 2m) \mid k \in [m], j \in J_r \}. \end{aligned}$$

La proposition qu'on veut démontrer découlera tout de suite.
La (3) est vraie pour $r = a$, par définition du modèle $\mathfrak{A}_{2m}$.
Pour $r = \emptyset$, nous avons que

$$\{ (k, (k+j) \bmod 2m) \mid k \in [m],\, j \in \emptyset \} = \emptyset\,.$$

Aussi, pour $r = r_0 \cup r_1$, nous avons

$$\begin{aligned}&\{ (k,(k+j) \bmod 2m) \mid k \in [m],\, j \in J_{r_0} \cup J_{r_1} \} \\ &\quad = \{ (k, (k+j) \bmod 2m) \mid k \in [m],\, j \in J_{r_0} \} \cup \{ (k, (k+j) \bmod 2m) \mid k \in [m],\, j \in J_{r_1} \} \\ &\quad = \widetilde{r_0} \cup \widetilde{r_1} = \widetilde{r}\,.\end{aligned}$$

Pour $r = 1$, nous avons

$$\{ (k, (k+j) \bmod 2m) \mid k \in [m],\, j \in \{ 0 \} \} = \{ (k, k) \mid k \in [m] \}\,.$$

Pour $r = r_0 \cdot r_1$, nous avons

$$\begin{aligned}&(k, k') \in R(r_0 \cdot r_1) \\ &\quad \text{ssi}\ \exists j\,, j_0 \in J_{r_0},\, j_1 \in J_{r_1},\, j = j_0 + j_1,\, k' = k + j \bmod 2m \\ &\quad \text{ssi}\ \exists j_0 \in J_{r_0},\, j_1 \in J_{r_1}\ \text{ t.q. }\ k' = k + j_0 + j_1 \bmod 2m \\ &\quad \text{ssi}\ \exists j_0 \in J_{r_0},\, k'' \in [m]\ \text{t.q.}\ k'' = k + j_0 \bmod 2m\ \text{ et }\ \exists j_1 \in J_{r_1}\ \text{ t.q. }\ k' = k'' + j_1 \bmod 2m \\ &\quad \text{ssi}\ \exists k''(k, k'') \in R(r_0)\ \text{et}\ (k'', k') \in R(r_1) \\ &\quad \text{ssi}\ (k, k') \in \widetilde{r_0 \cdot r_1}\,. \qquad \text{(Par hypothèse d'induction.)}\end{aligned}$$

Pour finir, si $r = r_0^*$, alors

$$\begin{aligned}&\{ (k,(k+j) \bmod 2m) \mid j \in J_{r_0^*} \} \\ &\quad = \{ (k, (k+j) \bmod 2m) \mid \exists n \geq 0\ \text{t.q.}\ j \in J_{r_0^n} \} \\ &\quad = \bigcup_{n\geq 0} R(r_0^n) = \bigcup_{n \geq 0} \widetilde{r_0^n} = \widetilde{r_0^*}\,.\end{aligned}$$

□

(ii). (2 points). Prouvez le fait suivant : *soient n, p tels que $n' > n$ implique $n' \in J_r$ ssi $n'+p \in J_r$; soit m un multiple de p tel que $n \leq m$; l'image de J_r modulo $2m$ est de la forme $A \cup B$ où $A \subseteq \{ 0, \ldots, n \}$ et $B \subseteq \{ 0, \ldots, 2m-1 \}$ est tel que $j \in B$ ssi $j + p \mod 2m \in B$.*

Solution. Nous pouvons écrire

$$J_r = A' \cup B'$$

où $A' \subseteq \{ 0, \ldots, n \}$ et $B' \subseteq \{ n+1, \ldots \}$ est tel que $n \in B'$ implique $n + p \in B'$. Posons

$$A = \{ n \bmod 2m \mid n \in A' \}\,, \qquad\qquad B = \{ n \bmod 2m \mid n \in B' \}\,.$$

Car l'image directe (d'un ensemble par une fonction) d'une réunion est la réunion des images directes, nous avons

$$\{ n \bmod 2m \mid n \in J_r \} = A \cup B\,.$$

Évidemment, on a $A \subseteq \{ 0, \ldots, n \}$, car $n \leq 2m$ (en effet on a $A = A'$). Il reste à montrer que $j \in B$ ssi $(j + p) \bmod 2m \in B$.
Supposons que $j \in B$: il existe $k \in B'$ tel que $j = k \bmod 2m$. Or $k + p \in B'$, et $j + p \bmod 2m = k + p \bmod 2m$: on a donc $j + p \bmod 2m \in B$.
Supposons que $j + p \in B$: il existe $k \in B'$ tel que $k \mod 2m = j + p$. Or $k + (\frac{2m}{p} - 1)p \in B'$ et du fait que

$$k + (\frac{2m}{p} - 1)p \bmod 2m = j + p + (\frac{2m}{p} - 1)p \bmod 2m = j + 2m \bmod 2m = j$$

il en découle que $j \in B$.
Remarque : nous avons utilisé dans nos calculs des propriétés fondamentales de l'arithmétique modulaire, comme par exemple le fait que $x + y \mod z = (x \mod z) + (y \mod z) \mod z$. □

Exercice 5. (8 points). Dans cet exercice nous proposons de comparer la logique temporelle ($\mathbb{LTL}, \mathbb{CTL}$) avec $\mathbb{PDL}$ et le μ-calcul. A ce fin, nous allons adapter le connecteur UNTIL[1] de la logique temporelle à la logique modale en définissant la sémantique de deux nouveaux connecteurs $\mathtt{U}^{\mathtt{s}}_a$, $\mathtt{U}^{\mathtt{w}}_a$.

Connecteur UNTIL fort (anglais : strong) par l'action atomique a :

$$s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi \;\text{ ssi }\; \text{il existe un calcul de la forme } s = s_0 \xrightarrow{a} s_1 \ldots \xrightarrow{a} s_n \text{ tel que } s_n \models \psi \text{ et } s_i \models \phi \text{ pour } i = 0, \ldots, n-1.$$

Connecteur UNTIL faible (anglais : weak) par l'action atomique a :

$$\begin{aligned} s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi \;\text{ ssi }\; & \text{il existe un calcul de la forme } s = s_0 \xrightarrow{a} s_1 \ldots \xrightarrow{a} s_n \text{ tel que } s_n \models \psi \text{ et } s_i \models \phi \text{ pour } i = 0, \ldots, n-1 \\ \text{ou } & \text{il existe un calcul infini par } a \text{ de } s \text{ sur lequel } \phi \text{ est toujours vraie}\,. \end{aligned}$$

(i). (3 points). Soit $U^s_{\phi,\psi}$ (resp. $U^w_{\phi,\psi}$) l'ensemble d'états tels que $s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$ (resp. $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$). Montrez que, pour $x = U^s_{\phi,\psi}, U^w_{\phi,\psi}$, on a

$$x = |\psi|_v \cup (|\phi|_v \cap \langle a \rangle x)\,.$$

Solution. Considérons d'abord $x = U^s_{\phi,\psi}$.
Nous allons nous intéresser à l'inclusion

$$U^s_{\phi,\psi} \subseteq |\psi|_v \cup (|\phi|_v \cap \langle a \rangle U^s_{\phi,\psi})\,.$$

Si $s \in U^s_{\phi,\psi}$ – c-à-d. $s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$ – alors il existe un entier $n \geq 0$ et un calcul $s = s_0 \xrightarrow{a} \ldots \xrightarrow{a} s_n$ avec $s_i \models \phi$ si $i < n$ et $s_n \models \phi$. Si $n = 0$, alors $s \models \psi$, et donc $s \in |\psi|_v$. Si $n > 0$, alors $s_0 \models \phi$ et il existe $s' = s_1$ tel que $s \xrightarrow{a} s'$ et évidemment $s' \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$, c'est à dire $s \in |\phi|_v \cap \langle a \rangle U^s_{\phi,\psi}$.
Pour l'autre inclusion,

$$|\psi|_v \cup (|\phi|_v \cap \langle a \rangle U^s_{\phi,\psi}) \subseteq U^s_{\phi,\psi}\,,$$

soit $s \in |\psi|_v \cup (|\phi|_v \cap \langle a \rangle U^s_{\phi,\psi})$.
Si $s \in |\psi|_v$, alors $s \models \psi$ et donc $s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$ (prenez le calcul de longueur 0). Si $s \in |\phi|_v \cap \langle a \rangle U^s_{\phi,\psi}$, alors $s \models \phi$ et il existe $s' \in U^s_{\phi,\psi}$ tel que $s \xrightarrow{a} s'$. Car $s' \in U^s_{\phi,\psi}$ – c'est à dire $s' \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$, il existe un calcul de la forme $s' = s_1 \xrightarrow{a} \ldots \xrightarrow{a} s_n$ (avec $n \geq 1$) avec $s_n \models \psi$ et $s_i \models \phi$ pour $1 \leq i < n$, et donc il existe un chemin de la forme

$$s = s_0 \xrightarrow{a} s' = s_1 \xrightarrow{a} \ldots \xrightarrow{a} s_n$$

satisfaisant les contraintes $s_i \models \phi$ pour $i = 0, \ldots, n-1$ et $s_n \models \phi$, ce qui témoigne que $s \in U^s_{\phi,\psi}$.

L'analyse pour $x = U^w_{\phi,\psi}$ se fait de façon analogue, en disant qu'un calcul de longueur ω témoin que $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$ est un calcul infini de la forme

$$s = s_0 \xrightarrow{a} s_1 \ldots \xrightarrow{a} s_n \xrightarrow{a} \ldots$$

avec $s_i \models \phi$ pour tout $i \geq 0$.
Plus précisément, étudions l'inclusion

$$U^w_{\phi,\psi} \subseteq |\psi|_v \cup (|\phi|_v \cap \langle a \rangle U^w_{\phi,\psi})\,.$$

Si $s \in U^w_{\phi,\psi}$ – c-à-d. $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$ – alors il existe $n \in \mathbb{N} \cup \{\, \omega \,\}$ et un calcul de longueur n témoin que $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$. Si $s \models \psi$ alors $s \in |\psi|_v$. Sinon on a nécessairement $n > 0$, et donc ce calcul est de la forme

$$s = s_0 \xrightarrow{a} s_1 \ldots$$

ce qui permet de dire qu'il existe $s' = s_1$ tel que $s \xrightarrow{a} s'$ et $s' \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$; car avec $s \models \phi$, alors $s \in |\phi|_v \cap \langle a \rangle U^w_{\phi,\psi}$.
Pour l'autre inclusion,

$$|\psi|_v \cup (|\phi|_v \cap \langle a \rangle U^w_{\phi,\psi}) \subseteq U^w_{\phi,\psi}\,,$$

[1] En français : jusque.

soit $s \in |\psi|_v \cup (|\phi|_v \cap \langle a\rangle U^w_{\phi,\psi})$. Si $s \in |\psi|_v$, alors $s \models \psi$ et donc $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$ (prenez le calcul de longueur 0). Si $s \in |\phi|_v \cap \langle a\rangle U^w_{\phi,\psi}$, alors $s \models \phi$ et il existe $s' \in U^w_{\phi,\psi}$ tel que $s \xrightarrow{a} s'$. Car $s' \in U^w_{\phi,\psi}$ – c'est à dire $s' \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$ – il existe $n \in \mathbb{N} \cup \{\,\omega\,\}$ et un calcul de longuer n

$$s' = s_1 \xrightarrow{a} \ldots s_k \xrightarrow{a} s_{k+1} \ldots$$

témoin de la relation $s' \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$. On obtient alors un calcul de longueur $1 + n$ (si $n = \omega$, alors $1 + \omega = \omega$)

$$s = s_0 \xrightarrow{a} s' = s_1 \xrightarrow{a} \ldots s_k \xrightarrow{a} s_{k+1} \ldots$$

témoin que $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$. ☐

(ii). (2 points). Argumentez que $s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$ ssi Eva possède une stratégie gagnante de $(s, \mu_x.\psi \vee (\phi \wedge \langle a\rangle x))$ dans le jeu $\mathcal{G}(\mathcal{M}, \mu_x.\psi \vee (\phi \wedge \langle a\rangle x))$. Argumentez que $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$ ssi Eva possède une stratégie gagnante de $(s, \nu_x.\psi \vee (\phi \wedge \langle a\rangle x))$ dans le jeu $\mathcal{G}(\mathcal{M}, \nu_x.\psi \vee (\phi \wedge \langle a\rangle x))$. Déduisez que $\mathtt{U}^{\mathtt{s}}_a$ et $\mathtt{U}^{\mathtt{w}}_a$ sont définissables dans le μ-calcul.

Solution. La preuve pour est analogue à la preuve de l'exercice 5 de l'examen de 2008 : un calcul de la forme

$$s_0 \xrightarrow{a} \ldots \xrightarrow{a} s_n$$

avec $s_i \models \phi$ pour $i < n$ et $s_n \models \psi$ donnera lieu à une stratégie gagnante pour Eva de $(s, \mu_x.\psi \vee (\phi \wedge \langle a\rangle x))$ dans $\mathcal{G}(\mathcal{M}, \mu_x.\psi \vee (\phi \wedge \langle a\rangle x))$, et viceversa.

Un calcul de la forme

$$s_0 \xrightarrow{a} \ldots \xrightarrow{a} s_k \xrightarrow{a} \ldots$$

où $s_i \models \phi$ pour $i < n$ et $s_n \models \psi$ si $n < \omega$ donnera lieu à une stratégie gagnante pour Eva de $(s, \nu_x.\psi \vee (\phi \wedge \langle a\rangle x))$ dans $\mathcal{G}(\mathcal{M}, \nu_x.\psi \vee (\phi \wedge \langle a\rangle x))$, et viceversa.

Remarquons la différence entre les deux jeux : dans le jeu $\mathcal{G}(\mathcal{M}, \nu_x.\psi \vee (\phi \wedge \langle a\rangle x))$ Eva a le droit de visiter une infinité de fois les positions de la forme (s_k, x), ce qui donne la possibilité d'avoir un chemin infini, qui ne se termine pas. Eva ne possède pas ce droit dans le jeu $\mathcal{G}(\mathcal{M}, \mu_x.\psi \vee (\phi \wedge \langle a\rangle x))$.
On a donc :

$$\begin{aligned} s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi \quad &\text{ssi} \quad s \in |\mu_x.\psi \vee (\phi \wedge \langle a\rangle x)|_v\,, \\ s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi \quad &\text{ssi} \quad s \in |\nu_x.\psi \vee (\phi \wedge \langle a\rangle x)|_v\,, \end{aligned}$$

ce qui montre que ces deux connecteurs sont définissables dans le μ-calcul, ☐

(iii). (1,5 points). Argumentez que le connecteur $\mathtt{U}^{\mathtt{s}}_a$ est définissable en $\mathbb{PDL}$ (avec test) : proposez une formule de $\mathbb{PDL}$ $\chi(x,y)$ telle que $s \models \chi(\phi,\psi)$ ssi $s \models \phi \mathtt{U}^{\mathtt{s}}_a \psi$, pour toute formule ϕ, ψ de $\mathbb{PDL}$.

Solution. Posons

$$\chi(x,y) = \langle ((?x) \cdot a)^* \rangle y\,.$$

☐

(iv). (1,5 points). Argumentez que le connecteur $\mathtt{U}^{\mathtt{w}}_a$ n'est pas définissable en $\mathbb{PDL}$ (avec test) ; c'est à dire, montrez qu'il n'existe pas une formule de $\mathbb{PDL}$ $\chi(x,y)$ telle que, pour toute formule ϕ, ψ de $\mathbb{PDL}$, $s \models \chi(\phi,\psi)$ ssi $s \models \phi \mathtt{U}^{\mathtt{w}}_a \psi$.

Solution. Supposons qu'une telle formule $\chi(x,y)$ existe. Observons que la formule $\chi(\top,\bot)$ est vraie dans un état ssi il existe un chemin infini par a. Donc, si cette formule existe, alors la propriété que tout chemin de s par a se termine (qui est la négation de la propriété qu'il existe un chemin infini par a de s) serait définissable. Nous avons vu en cours que cela n'est pas le cas. ☐

Automates sur les mots infinis et MSOL

Exercice 6. (2 points). Prouvez le fait suivant : *il n'existe pas un automate de Buchi déterministe qui reconnaît le langage*

$$abcde(a+b)^*a^\omega \,.$$

Solution. Nous allons argumenter par l'absurde. Supposons qu'un tel automate $\mathcal{A}$ existe, soit donc $\mathcal{A} = \langle Q, \{ \xrightarrow{a} \}_{a\in\Sigma}, q_0, F\rangle$. Soit q' l'unique état atteignable après avoir lu le mot *abcde* :

$$q' = q_0 abcde \,.$$

Considérons l'automate déterministe de Buchi $\mathcal{A}' = \langle Q, \{ \xrightarrow{a} \}_{a\in\Sigma}, q', F\rangle$. Soit $\sigma \in \mathcal{L}(\mathcal{A}')$, alors $abcde\sigma \in abcde(a+b)^*a^\omega$, et donc $\sigma \in (a+b)^*a^\omega$. Si par contre $\sigma \in (a+b)^*a^\omega$, alors le mot $abcde\sigma \in \mathcal{L}(\mathcal{A})$ et $\sigma \in \mathcal{L}(\mathcal{A}')$. Nous avons donc argumenté que

$$\mathcal{L}(\mathcal{A}') = (a+b)^*a^\omega \,,$$

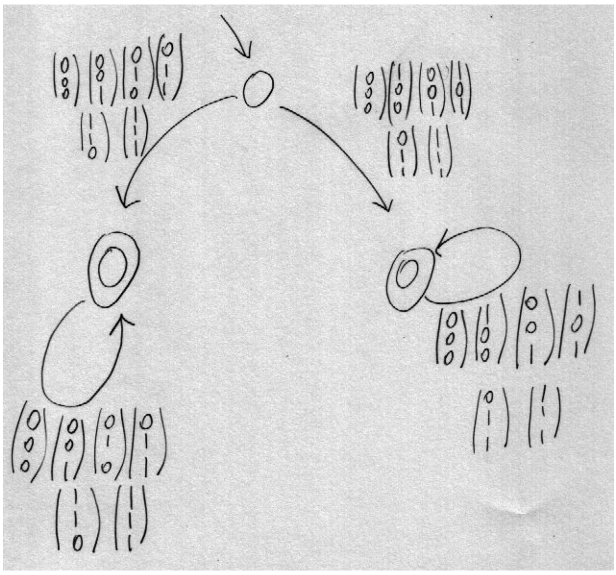
et en plus que $\mathcal{A}'$ est un automate déterministe. Cela est d'ailleurs une contradiction, car en cours nous avons vu qu'il n'existe pas une automate de Buchi déterministe reconnaissant le langage $(a+b)^*a^\omega$. $\square$

Exercice 7. (2 points). Construisez un automate de Buchi sur le langage $\Sigma = \{0,1\}^3$ qui reconnaît le langage

$$\{ \chi(S_1,S_2,S_3) \mid (S_1,S_2,S_3) \models X_1 \subseteq X_2 \vee X_2 \subseteq X_3 \} \,.$$

Argumentez que votre construction est correcte.

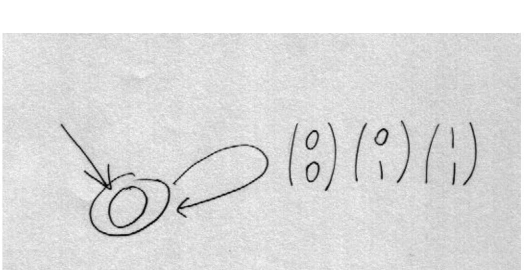
Solution. L'automate que nous proposons est le suivant :



Pour construire cet automate nous avons procédé comme suit.
Nous avons d'abord construit l'automate $\mathcal{A}$ reconnaissant le langage

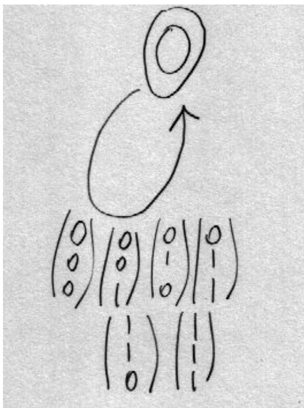
$$\{ \chi(S_1,S_2) \mid S_1,S_2 \models X \subseteq Y \} \,,$$

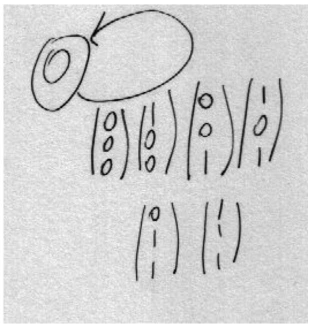
comme vu en cours :



En suite, nous avons ajouté une troisième (resp. première) composante vectorielle, de façon que l'automate $\mathcal{A}_1$ (resp. $\mathcal{A}_2$) reconnaisse le langage

$$\{\, \chi(S_1, S_2, S_3) \mid S_1, S_2, S_3 \models X_1 \subseteq X_2 \,\} \qquad \text{(resp.} \quad \{\, \chi(S_1, S_2, S_3) \mid S_1, S_2, S_3 \models X_2 \subseteq X_3 \,\})\,.$$





A partir des automates $\mathcal{A}_1, \mathcal{A}_2$, nous avons enfin construit l'automate reconnaissant la réunion des langages $\mathcal{L}(\mathcal{A}_1)$ et $\mathcal{L}(\mathcal{A}_2)$. □

Exercice 8. (2 points). Montrez que la relation d'ordre sur les entiers est définissable à partir de la relation de successeur en utilisant les quantificateurs de second ordre. C'est à dire, proposez une formule ϕ de MSOL – qui pourra bien avoir des occurrences du symbole de prédicat binaire S mais qui n'aura pas d'occurrences des symboles $<$ et $\leq$ – telle que $FV(\phi) = \{\, x, y \,\}$ et

$$\mathbb{N}, v \models \phi(x, y) \quad \text{ssi} \quad v(x) \leq v(y)\,.$$

Solution. La formule suivante dit que $y \in \{\, z \mid x \leq z \,\}$:

$$\begin{array}{rl} \phi(x,y) := \exists X(& X(x) \\ & \wedge \\ & \forall z\,(\,zSx \implies \neg X(z)) \\ & \wedge \\ & \forall z, w\,(\,X(z) \wedge zSw \implies X(w)\,) \\ & \wedge \\ & X(y) \\ &)\,. \end{array}$$

□