M1 - T.D. APS – CCS et Vérification

Exercice 1 Que peut-on trouver dans la variable x après l'exécution du programme suivant ?
$x := 10;\ \big((x := x \times 2; x := x - 11; x := x + 2) \parallel x := x - 5\big)$ ♢

Exercice 2 Parmi les expressions suivantes, lesquelles sont des expressions CCS syntaxiquement correctes ? Justifiez les réponses. A, B sont des noms de processus et a, b des noms de canaux.

1. $a.b.A + B$
2. $(a.NIL + \bar{a}A) \setminus \{a, b\}$
3. $(a.NIL \parallel \bar{a}A) \setminus \{a, \tau\}$
4. $a.A + [a/b]$
5. $a.\tau.\tau.A + NIL$
6. $(a.B + b.B)[a/b, b/a]$
7. $(a.B + \tau.B)[a/\tau, b/a]$
8. $(a.NIL + \bar{a}A) \parallel B$
9. $(a.NIL + \bar{a}A).B$
10. $(a.NIL + \bar{a}A) + B$
11. $(Nil \parallel Nil) + Nil$ ♢

Exercice 3 On considère le sytème de transition ST dessiné ci-dessous.

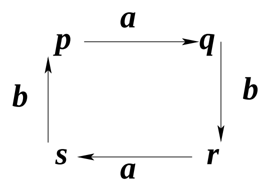

Figure 1

Décrivez-le comme un triplet $(Proc, Act, T)$. ♢

Exercice 4 On considère le processus CCS (machine à café simple) défini par

$$M \stackrel{\text{def}}{=} e.c.\bar{p}.M$$

Définissez un processus (machine à café voleuse) qui décrive une machine à café qui peut

– soit se comporter commme M
– soit prendre la pièce et ne rien donner ♢

Exercice 5 Soit $(Proc, Act, T)$ un ST avec $Proc$ et Act finis.

1. Montrez que T est aussi fini.
2. Dessinez un exemple de ST à 4 états et 2 actions.
3. Ecrivez la définition de votre ST comme programme CCS séquentiel.
4. Montrez que tout ST fini peut être décrit comme un programme CCS séquentiel. ♢

Exercice 6 Soient $A = a.Nil + b.Nil$ et $B = \bar{a}.B + b.B$. Soient $P \stackrel{\text{def}}{=} A \parallel B$ et $Q \stackrel{\text{def}}{=} (A \parallel B)\setminus\{a\}$.

1. Donnez toutes les transitions de la forme $\xrightarrow{x}$ avec $x \in \{a, b, \bar{a}, \tau\}$ de P (resp. Q) en les justifiant par la sémantique SOS de CCS.
2. Dessinez un ST pour P (resp. Q).
3. P (resp. Q) peut-il bloquer ?
4. Mêmes questions en remplaçant B par $B' \stackrel{\text{def}}{=} \bar{a}.b.B'$. ♢

Exercice 7 Soit $A \stackrel{\text{def}}{=} b.a.B$. Vérifiez que les dérivations suivantes sont correctes :

- $(A \parallel \bar{b}.a.B) + (\bar{b}.A)[a/b] \xrightarrow{\bar{b}} (A \parallel a.B)$

T.S.V.P.

- $(A \parallel \bar{b}.a.B) + (\bar{b}.A)[a/b] \xrightarrow{\bar{a}} A[a/b]$
- $(A \parallel \bar{b}.Nil) \setminus \{b\} \xrightarrow{\tau} (a.B \parallel Nil) \setminus \{b\}$ $\diamondsuit$

EXERCICE 8 On considère le processus CCS S défini par les équations :

$$M \stackrel{\text{def}}{=} e.\bar{c}.M$$
$$I \stackrel{\text{def}}{=} ex.\bar{e}.c.I$$
$$S \stackrel{\text{def}}{=} (M \parallel I) \setminus \{e, c\}$$

Dessinez le système de transition correspondant. $\diamondsuit$

EXERCICE 9 1. Dessinez un ST pour le processus A défini par $A \stackrel{\text{def}}{=} (a.A) \setminus \{b\}$. le ST obtenu doit avoir une infinité d'états.

2. Trouvez un processus CCS qui peut être décrit par un ST fini, et qui a le même comportement (intuitivement) que A. $\diamondsuit$

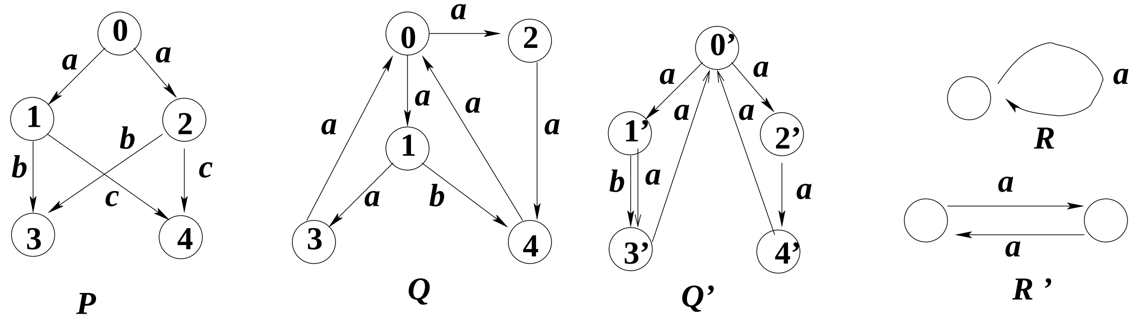

Figure 2

EXERCICE 10 On considère le ST P de la figure 2. Dans quels états de P les formules suivantes de HML sont-elles satisfaites ?

1. $[a]\ ([a]tt \vee [a]ff)$
2. $[a]\ ([b]tt \wedge [c]tt)$
3. $[a]\ ([a]ff \wedge [c]tt)$ $\diamondsuit$

EXERCICE 11 On considère le ST Q de la figure 2. Dans quels états de Q les formules suivantes de HML sont-elles satisfaites ?

1. $\langle a\rangle tt$
2. $\langle b\rangle tt$
3. $[a]ff$
4. $[b]ff$
5. $[a]\langle b\rangle tt$
6. $\langle a\rangle\ \langle b\rangle tt$
7. $\langle b\rangle\ \langle b\rangle tt$
8. $[a]\langle a\rangle[a][b]ff$
9. $\langle a\rangle\ (\langle a\rangle tt \wedge \langle b\rangle tt)$
10. $[a]\ (\langle a\rangle tt \vee \langle b\rangle tt)$
11. $\langle a\rangle\ ([b][a]ff \wedge \langle b\rangle tt)$
12. $\langle a\rangle\ \big([a](\langle a\rangle tt \wedge [b]ff) \wedge \langle b\rangle ff\big)$
13. $[a][a][b]ff$ $\diamondsuit$

EXERCICE 12 On considère le ST R de la figure 2. Les formules suivantes de HML sont-elles satisfaites par R ?

1. $\langle a \rangle \mathit{tt}$
2. $[a] \mathit{ff}$
3. $[a]\ (\langle a \rangle \mathit{tt} \wedge [b] \mathit{ff})$
4. $[a]\ (\langle b \rangle \mathit{tt} \vee [a] \mathit{ff})$

Est ce que R et R' satisfont les mêmes formules HML ? $\diamondsuit$

Exercice 13 Pour chacune de formules HML ci-dessous donnez si possible un ST qui la satisfasse.
1. $\langle a \rangle \mathit{tt} \wedge [a] \mathit{ff}$ (soit F_1 cette formule)
2. $\langle a \rangle [b] (\langle a \rangle \mathit{tt} \wedge [a] \mathit{ff})$ (soit F_2 cette formule $F_2 = \langle a \rangle [b] F_1$)
3. $F_2 \wedge \bigwedge_{a \in Act} [a] \langle b \rangle \mathit{tt}$
4. $F_2 \wedge \bigwedge_{a \in Act} [a] \bigvee_{b \in Act} \langle b \rangle \mathit{tt}$ $\diamondsuit$

Exercice 14 1. Interprétez la formule :

$\bigvee_{a \in Act} \langle a \rangle \mathit{tt} \wedge \bigwedge_{a \in Act} [a] \big(\bigvee_{a \in Act} \langle a \rangle \mathit{tt} \wedge \bigwedge_{a \in Act} [a] (\bigvee_{a \in Act} \langle a \rangle \mathit{tt} \wedge \bigwedge_{a \in Act \setminus \{a\}} [a] \mathit{ff}) \big)$

2. Donnez un ST qui la satisfasse.
3. Donnez un ST ayant le plus petit nombre d'états possible qui la satisfasse. $\diamondsuit$

Exercice 15 Trouvez un ST qui satisfasse les trois propriétés suivantes.
1. $\langle a \rangle\ (\langle b \rangle \langle c \rangle \mathit{tt} \wedge \langle c \rangle \mathit{tt})$
2. $\langle a \rangle \langle b \rangle\ ([a] \mathit{ff} \wedge [b] \mathit{ff} \wedge [c] \mathit{ff})$
3. $[a] \langle b \rangle\ ([c] \mathit{ff} \wedge \langle a \rangle \mathit{tt})$ $\diamondsuit$

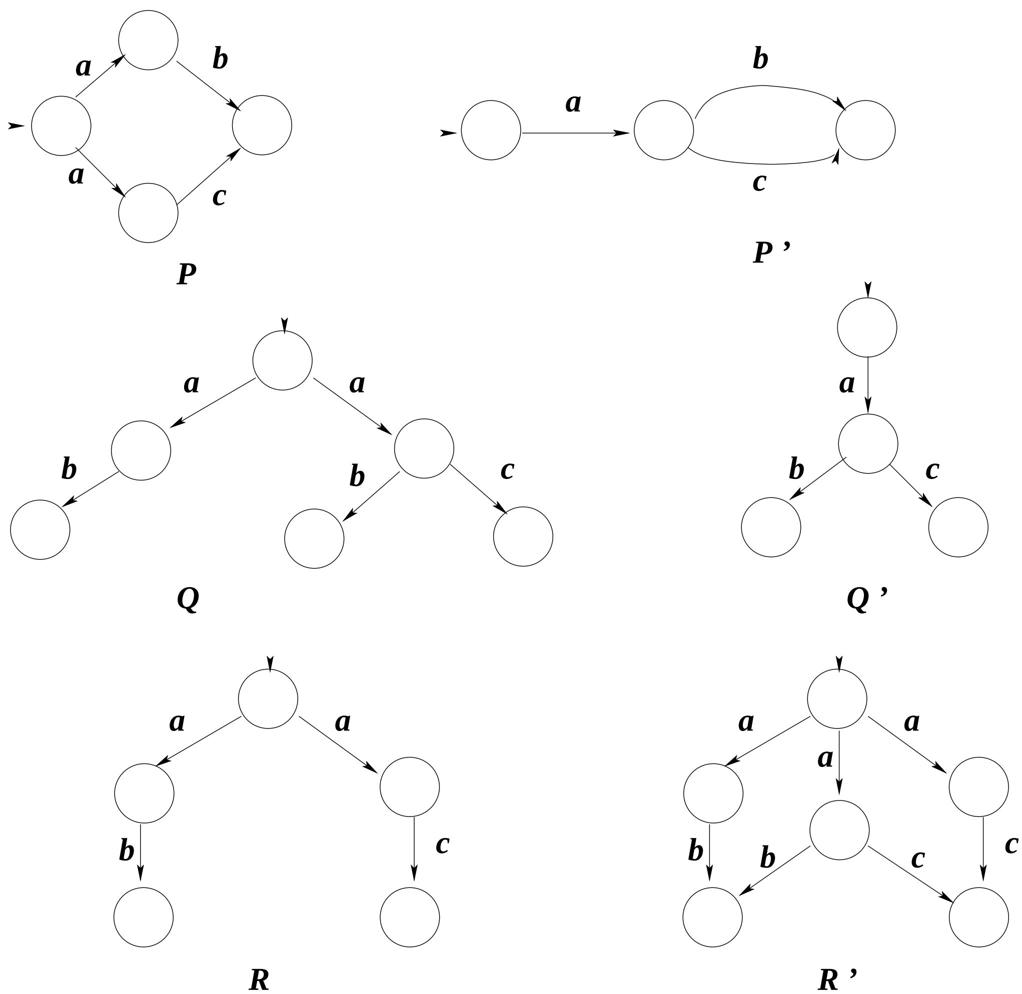

Figure 3

EXERCICE 16 Donnez une formule HML qui distingue les ST P et P' de la figure 3 en étant satisfaite par P et pas par P'. $\diamondsuit$

EXERCICE 17 Donnez une formule HML qui distingue les ST Q et Q' de la figure 3 en étant satisfaite par Q' et pas par Q. $\diamondsuit$

EXERCICE 18 Donnez une formule HML qui distingue les ST R et R' de la figure 3 en étant satisfaite par R' et pas par R. $\diamondsuit$

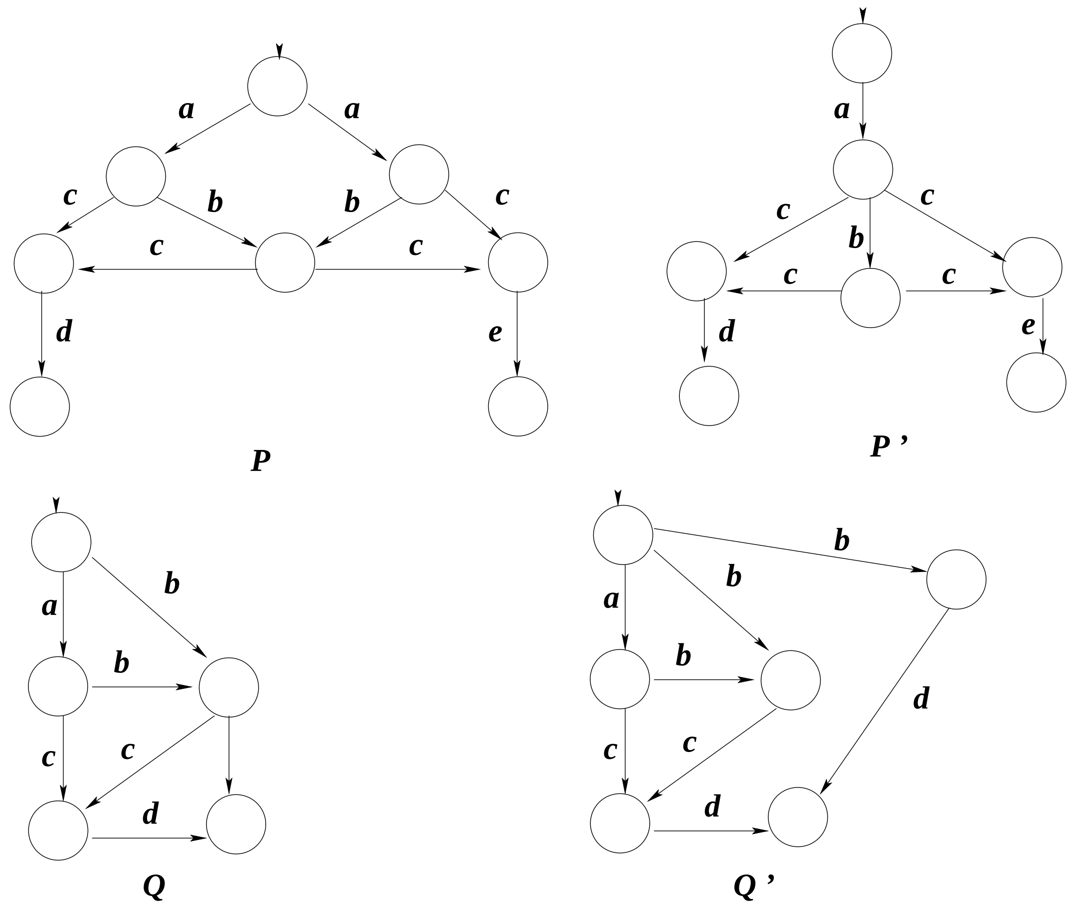

Figure 4

EXERCICE 19 Donnez une formule HML qui distingue les ST P et P' de la figure 4. $\diamondsuit$

EXERCICE 20 Donnez une formule HML qui distingue les ST Q et Q' de la figure 4. $\diamondsuit$

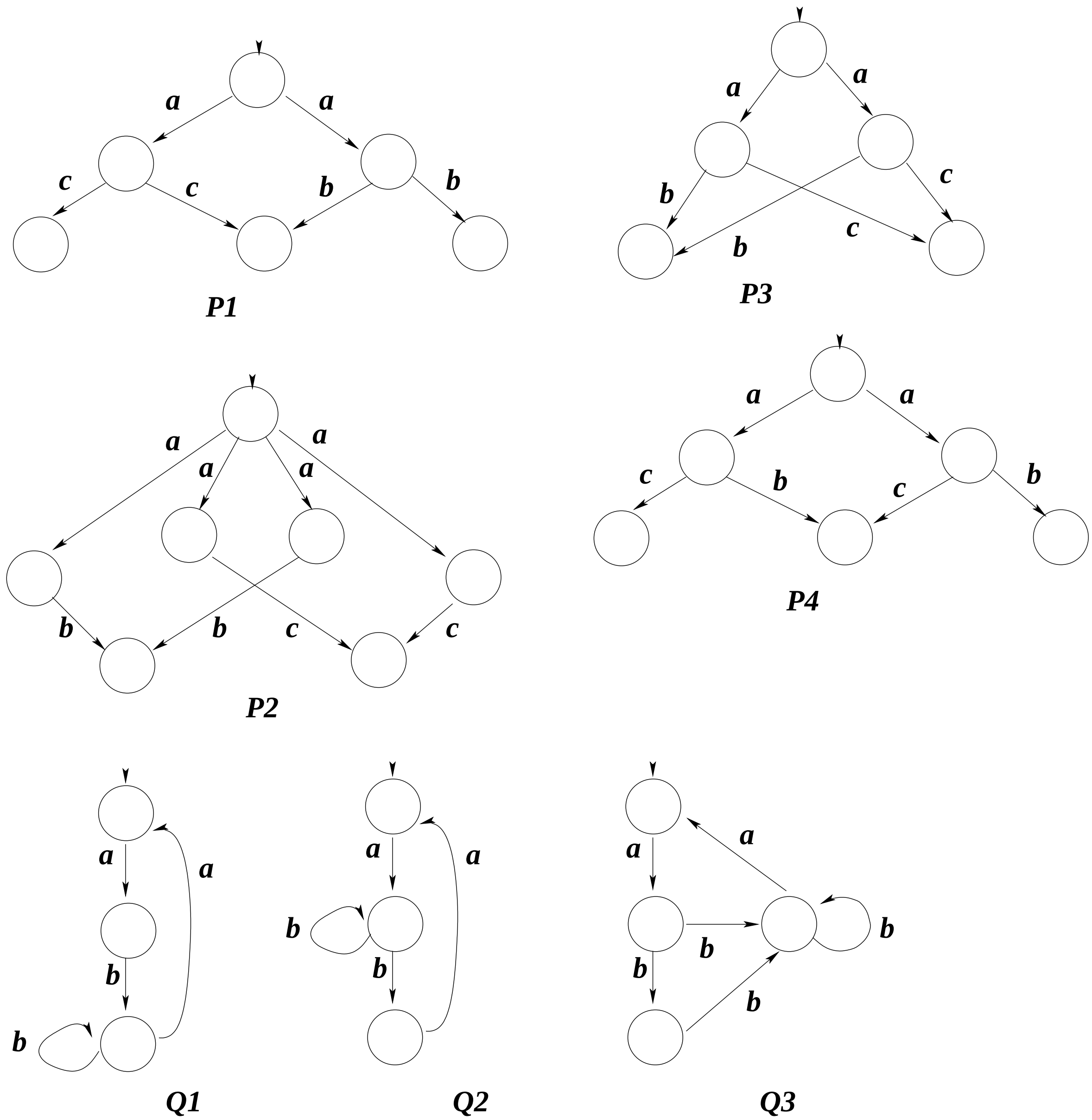

Figure 5

Exercice 21 Est-il possible de donner des formules HML qui distinguent les ST $P1$, $P2$, $P3$ et $P4$ de la figure 5 ? $\diamondsuit$

Exercice 22 Donnez trois formules HML qui distinguent les ST $Q1$, $Q2$ et $Q3$ de la figure 5 deux à deux. $\diamondsuit$

Exercice 23 La profondeur d'une formule HML est définie par
(B) $prof(tt) = prof(ff) = 0$
(I) $prof(F \wedge G) = prof(F \vee G) = \max\{prof(F), prof(G)\}$
(I) $prof([a]F) = prof(\langle a \rangle F) = prof(F) + 1$

Trouvez deux processus CCS qui ne sont pas distinguables par une formule de profondeur 1 mais qui sont distinguables par une formule de profondeur 2 ou plus. $\diamondsuit$

Exercice 24 Donnez des formules HTML qui expriment les propriété suivantes :

1. On peut faire un a suivi par un b puis par un c.
2. Si on peut faire un a, il ne peut être suivi ni d'un b ni d'un c.
3. Si on peut faire un a et si un b est aussi possible, alors le a ne peut pas être suivi d'un b.
4. On peut faire un a ou un b, mais après avoir fait le a on ne peut plus faire de b. $\diamondsuit$

Bisimulations

Exercice 25 1. Les processus Ms et Mn de la figure 6 sont-ils fortement bisimilaires ?

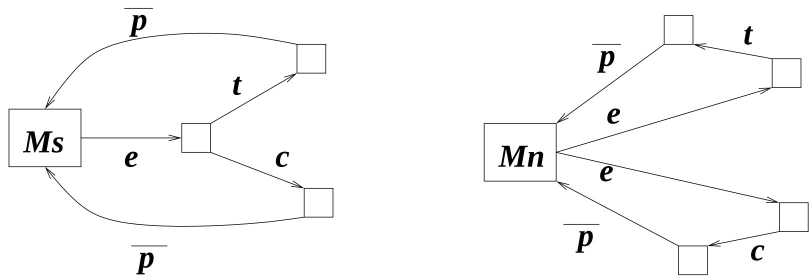

Figure 6

2. Les processus R et R' de la figure 2 sont-ils fortement bisimilaires ?

3. Montrez que les processus $P1$ et $P2$, (resp. $P3$ et $P4$) de la figure 5 sont fortement bisimilaires. $\diamondsuit$

Exercice 26 1. Montrez que $\sim = \cup\{R | R$ est une bisimulation forte $\}$ est une relation d'équivalence (réflexive, symétrique et transitive).

2. Montrez que $\sim$ est la plus grande bisimulation forte. $\diamondsuit$

Exercice 27 1. On considère les processus P et Q définis par :

$P \xrightarrow{a} 0$, $P \xrightarrow{a} 1$ et $1 \xrightarrow{b} 2$

$Q \xrightarrow{a} 3$, $3 \xrightarrow{b} 4$

P et Q sont-ils fortement bisimilaires ?

2. Une relation binaire $R \subseteq Proc \times Proc$ est une simulation ssi pour tous $(s,t) \in R$ et pour tout $a \in Act$:

– si $s \xrightarrow{a} s'$ alors $t \xrightarrow{a} t'$ pour un t' tel que $(s', t') \in R$

P est simulé par Q (notation $P < Q$) ssi il existe une simulation R telle que $(P,Q) \in R$.

Montrez que $P \sim Q$ implique $P < Q$ et $Q < P$. La réciproque est-elle vraie ? $\diamondsuit$

Exercice 28 Le but de cet exercice est de montrer que sur les processus qui ne sont pas à branchement fini, $\sim \neq \sim_{omega}$. Soit $P = \sum_{n\in\mathbb{N}} a^n.NIL$ alors montrer que $P \sim_{omega} \sum_{n\in\mathbb{N}} a^n.NIL + a^\omega$ mais $P \not\sim \sum_{n\in\mathbb{N}} a^n.NIL + a^\omega$. $\diamondsuit$

Exercice 29 1. Les processus $\tau.NIL + \tau.a.NIL$ et $a.NIL$ sont-ils fortement bisimilaires ? faiblement bisimilaire ?

2. Montrer que $a.NIL + b.NIL \not\approx a.NIL + \tau.b.NIL \not\approx \tau.a.NIL + \tau.b.NIL \not\approx a.NIL + b.NIL$.

3. Montrer que $a.NIL \approx \tau.a.NIL \approx a.NIL + \tau.a.NIL$.

4. On abrège $a.NIL$ en a. Montrer que $a.(b + \tau.c) \approx a.(b + \tau.c) + a.c$ $\diamondsuit$

Exercice 30 Les processus Q et Q' de la figure 2 sont-ils fortement bisimilaires ? $\diamondsuit$

Exercice 31 On considère les processus P et Q définis par :

$P = a.P_1 \quad P_1 = b.P + c.P$

$Q = a.Q_1 \quad Q_1 = b.Q_2 + c.Q \quad Q_2 = a.Q_3 \quad Q_3 = b.Q + c.Q_2$

Montrer qu'ils fortement bisimilaires. $\diamondsuit$

Exercice 32 On considère les processus de la figure 7. Est-ce que $S \sim T$? $S \sim U$? $S \sim V$?

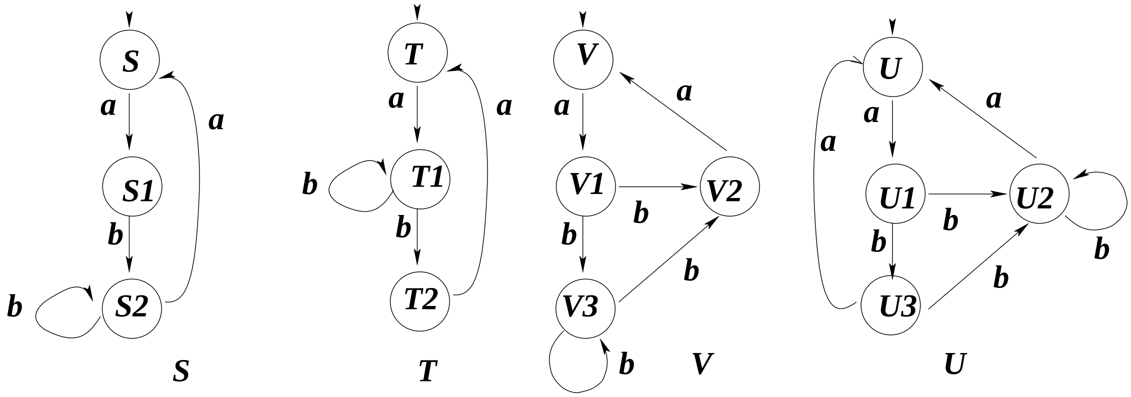

Figure 7

Donner une stratégie universelle pour l'attaquant (si non bisimilaires) ; sinon (bisimilaires) donner soit une stratégie universelle pour le défenseur, soit définir explicitement la bisimulation. $\diamondsuit$

1. $x = 1$ ou $x = 6$, 4 exécutions possibles.

2. toutes correctes sauf

3. faux on n'utilise pas τ ds une restriction
4. faux, on ne renomme que des expressions correctes
7. faux, τ doit être renommé en τ
9. faux, on ne peut préfixer que par des actions ($P; Q$ interdit en CCS)

3. $Proc = \{p, q, r, s\}$ $\quad Act = \{a, b\}$ $\quad T = \{(p, a, q)\ ,\ (r, a, s)\ ,\ (q, b, r)\ ,\ (s, b, p)\}$

4. $M' \stackrel{\text{def}}{=} e.c.\bar{p}.M' + e.M'$

ou encore (si on suppose un CCS asynchrone où la transition $fail$ peut se déclencher avant la communication sur le canal c,

$M' \stackrel{\text{def}}{=} e.(c.\bar{p}.M' + M' + fail.Nil) + fail.Nil.$

ou encore $M'' \stackrel{\text{def}}{=} M + e.M''$

Remarquer que M' et M'' ont des comportements différents (si M'' décide de devenir honnête elle le reste, alors que M' peut à chaque étape recommencer à voler.

5. 1. Il y a au maximum $2^{|Proc| \times |Act|}$ éléments dans T.

2. Pour le processus de la figure 1, on a :

$$p \stackrel{\text{def}}{=} a.q\ ,\ q \stackrel{\text{def}}{=} b.r\ ,\ r \stackrel{\text{def}}{=} a.s\ ,\ s \stackrel{\text{def}}{=} b.p$$

3. Un autre exemple

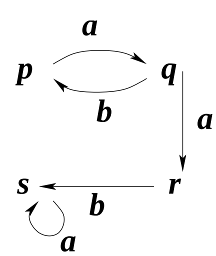

Figure 8

et ses équations CCS :

$$p \stackrel{\text{def}}{=} a.q\ ,\ q \stackrel{\text{def}}{=} b.p + a.r\ ,\ r \stackrel{\text{def}}{=} b.s\ ,\ s \stackrel{\text{def}}{=} a.s$$

4. Pour chaque $p \in Proc$ on ajoute la définition d'un nouveau processus p :

- si $p \not\longrightarrow$ on pose $p \stackrel{\text{def}}{=} Nil$, sinon
- si $p \xrightarrow{a_1} p_1$, $p \xrightarrow{a_2} p_2, \ldots, p \xrightarrow{a_n} p_n$, on pose $p \stackrel{\text{def}}{=} a_1 p_1 + a_2.p_2 + \cdots + a_n.p_n$

6. 1. $P \xrightarrow{a} Nil \parallel B$ (ACT et COM1), $P \xrightarrow{b} Nil \parallel B$ (ACT et COM1), $P \xrightarrow{\bar{a}} P$ (ACT et COM2), $P \xrightarrow{b} P$ (ACT et COM2), $P \xrightarrow{\tau} Nil \parallel B$ (ACT, ACT et COM3)

Pour $Q \stackrel{\text{def}}{=} (A \parallel B) \setminus \{a\}$, on n'a plus que 3 transitions (celles sans $a, \bar{a}$)

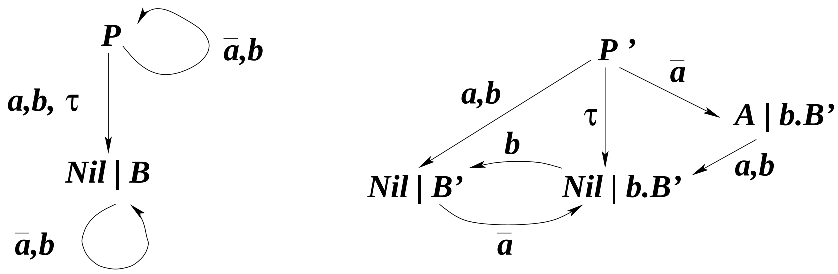

Figure 9

pour Q supprimer les transitions avec $a, \bar{a}$ et rajouter la restriction par a.

3. ni P ni Q ne bloquent.

4. Posons $P' \stackrel{\text{def}}{=} A \parallel B'$ et $Q' \stackrel{\text{def}}{=} (A \parallel B') \setminus \{a\}$.

$P' \xrightarrow{a} Nil \parallel B'$ (ACT et COM1), $P' \xrightarrow{b} Nil \parallel B'$ (ACT et COM1), $P' \xrightarrow{\bar{a}} A \parallel b.B'$ (ACT et COM2), $P' \xrightarrow{\tau} Nil \parallel b.B'$ (ACT, ACT et COM3)

Pour $Q' \stackrel{\text{def}}{=} (A \parallel B') \setminus \{a\}$, on n'a plus que 2 transitions (celles sans $a, \bar{a}$)

P' ne bloque jamais, par contre Q' peut arriver a $Nil \parallel B'$ qui est bloquant.

7.

- $(A \parallel \bar{b}.a.B) + (\bar{b}.A)[a/b] \xrightarrow{\bar{b}} (A \parallel a.B)$

par ACT $\bar{b}.a.B \xrightarrow{\bar{b}} a.B$

par COM2 $A \parallel \bar{b}.a.B \xrightarrow{\bar{b}} A \parallel a.B$

par SUM1 $(A \parallel \bar{b}.a.B) + (\bar{b}.A)[a/b] \xrightarrow{\bar{b}} (A \parallel a.B)$

- $(A \parallel \bar{b}.a.B) + (\bar{b}.A)[a/b] \xrightarrow{\bar{a}} A[a/b]$

par ACT $\bar{b}.A \xrightarrow{\bar{b}} A$

par REL $\bar{b}.A[a/b] \xrightarrow{\bar{a}} A[a/b]$

par SUM2 $(A \parallel \bar{b}.a.B) + (\bar{b}.A)[a/b] \xrightarrow{\bar{a}} A[a/b]$

- $(A \parallel \bar{b}.Nil) \setminus \{b\} \xrightarrow{\tau} (a.B \parallel Nil) \setminus \{b\}$

par ACT $\bar{b}.Nil \xrightarrow{\bar{b}} Nil$ sera utilisé ensuite avec COM3

par ACT $b.a.B \xrightarrow{b} a.B$

par CON puisque $A \stackrel{\text{def}}{=} b.a.B$, et $b.a.B \xrightarrow{b} a.B, \quad A \xrightarrow{b} a.B$

par COM3 $(A \parallel \bar{b}.Nil) \xrightarrow{\tau} (a.B \parallel Nil)$

par RES puisque $\{\tau, \bar{\tau}\} \notin \{b\}, \quad (A \parallel \bar{b}.Nil) \setminus \{b\} \xrightarrow{\tau} (a.B \parallel Nil) \setminus \{b\}$

8.

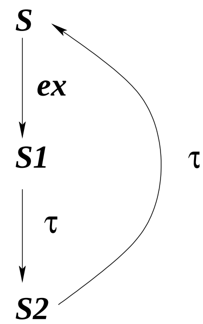

Figure 10

où $S1 = (M \parallel \bar{e}.c.I) \setminus \{e, c\}$
et $S2 = (\bar{c}.M \parallel c.I) \setminus \{e, c\}$

9. 1. ST pour $A \stackrel{\text{def}}{=} (a.A) \setminus \{b\}$.
$A \xrightarrow{a} A \setminus \{b\} \xrightarrow{a} (A \setminus \{b\}) \setminus \{b\} \xrightarrow{a} \big((A \setminus \{b\}) \setminus \{b\}\big) \setminus \{b\} \xrightarrow{a} \cdots$
2. On peut définir $B \stackrel{\text{def}}{=} a.B$ qui correspond à un ST fini avec le même comportement que A.

10. La formule $[a]tt$ est toujours vraie, pour tout a et tout état. Elle est donc équivalente à tt ; les 2 premières formules dont donc vraies dans tous les états du ST.

Pour la 3eme formule, $[a]ff$ exprime qu'on ne peut pas faire de a-transition elle est vraie dans les états 1,2,3,4 ; la formule $[c]tt$ est toujours vraie, donc la formule $([a]ff \wedge [c]tt)$ est vraie dans les états 1,2,3,4 ; finalement, $[a]\ ([a]ff \wedge [c]tt)$ est vraies dans tous les états du ST. Elle exprime qu'on ne peut pas faire 2 a-transitions consécutives et est équivalente à $[a]\ [a]ff$.

11.
1. $\langle a\rangle tt$ vraie dans 0,1,2,3,4.
Autre manière de dire la même chose $[\![\langle a\rangle tt]\!] = \{0, 1, 2, 3, 4\}$
2. $\langle b\rangle tt$ vraie dans 1
3. $[a]ff$ toujours fausse
4. $[b]ff$ vraie dans 0,2,3,4
5. $[a]\langle b\rangle tt$ toujours fausse ($\langle b\rangle tt$ vraie dans 1)
6. $\langle a\rangle\ \langle b\rangle tt$ vraie dans 0
7. $\langle b\rangle\ \langle b\rangle tt$ toujours fausse
8. $[a]\langle a\rangle[a][b]ff$ vraie ds 0,3,4 ;
$[b]ff$ vraie dans 0,2,3,4 ; $[a][b]ff$ vraie dans les états dont tous les A-successeurs sont dans 0,2,3,4 et dc $[a][b]ff$ vraie dans 1,2,3,4 : $\langle a\rangle[a][b]ff$ vraie ds 0,1,2.
9. $\langle a\rangle\ (\langle a\rangle \wedge \langle b\rangle tt)$ vraie ds 0 ; $\langle a\rangle tt$ vraie dans 0,1,2,3,4 et $\langle b\rangle tt$ vraie dans 1 ; $(\langle a\rangle \wedge \langle b\rangle tt)$ vraie ds 1.
10. $[a]\ (\langle a\rangle tt \vee \langle b\rangle tt)$ vraie toujours.
$\langle a\rangle tt$ toujours vraie et $\langle b\rangle tt$ vraie ds 1 ; $(\langle a\rangle tt \vee \langle b\rangle tt)$ toujours vraie.
11. $\langle a\rangle\ ([b][a]ff \wedge \langle b\rangle tt)$ toujours fausse.
$[a]ff$ toujours faux et $\langle b\rangle tt$ vraie ds 1 ; $[b][a]ff$ vrai ds 0, 2, 3, 4 ; $([b][a]ff \wedge \langle b\rangle tt)$ toujours faux.

12. $\langle a\rangle\ \big([a](\langle a\rangle tt \wedge [b]ff) \wedge \langle b\rangle ff\big)$ toujours faux.

$\langle a\rangle tt$ toujours vrai ; $[b]ff$ vrai ds 0, 2, 3, 4 ; $\langle b\rangle ff$ toujours faux ; $\langle a\rangle tt \wedge [b]ff$ vrai ds 0, 2, 3, 4 ; $([a](\langle a\rangle tt \wedge [b]ff)$ vrai ds 1, 2, 3, 4 ; $\big([a](\langle a\rangle tt \wedge [b]ff) \wedge \langle b\rangle ff\big)$ toujours faux.

13. $[a][a][b]ff$ vrai ds 0, 1, 2

$[a][b]ff$ vrai ds 1, 2, 3, 4 et dc on doit partir de 0, 1, 2 pr que ts les a-successeurs soient ds 1, 2, 3, 4.

12.

1. $\langle a\rangle tt$ oui
2. $[a]ff$ non
3. $[a]\ (\langle a\rangle tt \wedge [b]ff)$ oui(les 2 ss-formules sont vraies).
4. $[a]\ (\langle b\rangle tt \vee [a]ff)$ non (les 2 ss-formules sont fausses).

OUI (ST R et R' sont bisimilaires).

13.

1. $\langle a\rangle tt \wedge [a]ff$ (soit F_1 cette formule) impossible la première partie exprime que il y a une a-transition et la seconde partie interdit qu'il y ait une a-transition.
2. $\langle a\rangle[b](\langle a\rangle tt \wedge [a]ff)$ (soit F_2 cette formule $F_2 = \langle a\rangle[b]F_1$) Il doit y avoir une a-transition et après cette transition $[b](\langle a\rangle tt \wedge [a]ff)$ doit être vraie, i.e. pas de b-transition: il suffit de prendre le ST réduit à $0 \xrightarrow{a} 1$
3. $F_2 \wedge \bigwedge_{a\in Act}[a]\langle b\rangle tt$

$\bigwedge_{a\in Act}[a]\langle b\rangle tt$ exige qu'après tout état atteint en une seule transition depuis l'état initial, on puisse faire une b-transition ; cela contredit F_2 qui dit que il y a une a-transition après qui il n'y a pas de b-transition ; pas de ST qui satisfasse cette formule.

4. $\bigwedge_{a\in Act}[a]\bigvee_{b\in Act}\langle b\rangle tt$ exige qu'après tout état atteint en une seule transition depuis l'état initial, on puisse faire une b-transition pour un b dans Act ; F_2 dit que il y a une a-transition après qui il n'y a pas de b-transition : il suffit de faire une a-transition depuis l'état initial et ensuite une transition autre que b. $0 \xrightarrow{a} 1 \xrightarrow{c} 2$.

14. 1. $\bigvee_{a\in Act}\langle a\rangle tt \wedge \bigwedge_{a\in Act}[a]\big(\bigvee_{a\in Act}\langle a\rangle tt \wedge \bigwedge_{a\in Act}[a](\bigvee_{a\in Act}\langle a\rangle tt \wedge \bigwedge_{a\in Act\setminus\{a\}}[a]ff)\big)$

On peut faire 3 transitions consécutives, et la troisième transition doit être une a-transition.

2. $0 \xrightarrow{c} 1 \xrightarrow{b} 2 \xrightarrow{a} 3$

3. $0 \xrightarrow{a} 0$

15. 1. on doit pouvoir faire abc et ac

2. il y a un ab après qui on ne peut faire ni a ni b ni c

3. après tout a on peut faire un b après lequel pas de c mais un a doit être possible

On ne peut pas fusionner les b car apès les b on demande des choses contradictoires. (VOIR CORRIGE)

16. $\langle a\rangle[b]ff$

17. $[a]\langle c\rangle tt$

18. $\langle a\rangle\ (\langle b\rangle tt \wedge \langle c\rangle tt)$

19. $[a]\langle c\rangle\langle e\rangle tt$ est satisfaite par P' et pas par P.

20. $\langle b\rangle\ (\langle c\rangle tt \wedge \langle d\rangle tt)$ est satisfaite par Q et pas par Q'.

21. On ne peut pas distinguer $P1$, $P2$ (bisimilaires) ni $P3$ et $P4$ (bisimilaires).
$\langle a\rangle\ (\langle b\rangle tt \wedge \langle c\rangle tt)$ est satisfaite par $P3$ et $P4$, mais pas par $P1$ ni $P2$.

22.
$\langle a\rangle\ \langle b\rangle [b] ff$ est satisfaite par $Q2$ et pas par $Q1$.
$[a]\ [b]\ (\langle a\rangle tt \wedge \langle b\rangle tt)$ est satisfaite par $Q1$ et pas par $Q3$.
$\langle a\rangle\ \langle b\rangle\ (\langle a\rangle tt \wedge \langle b\rangle tt)$ est satisfaite par $Q3$ et pas par $Q2$

23. $P = a.P$ et $Q = a.Q + a.a.NIL$. les formules de profondeur 1 sont :$\langle a\rangle tt$ ou $[a]tt$ ou $\langle a\rangle ff$ ou $[a]\ [a]ff$: et elles sont satisfaites (ou non satisfaites) en même temps par P et Q. Une formule de profondeur 2 qui distingue P et Q est : $F = \langle a\rangle\ \langle a\rangle\ [a]ff$ qui est satisfaite par Q mais pas par P (puisque P ne s'arrête jamais.

24.
1. On peut faire un a suivi par un b puis par un c.
   $\langle a\rangle\ \langle b\rangle\ \langle c\rangle tt$
2. Si on peut faire un a, il ne peut être suivi ni d'un b ni d'un c.
   $[a]\ ([b]ff \wedge [c]ff$
3. Si on peut faire un a et si un b est aussi possible, alors le a ne peut pas être suivi d'un b.
   $\langle a\rangle\ [b]ff \wedge [b]ff$
4. On peut faire un a ou un b, mais après avoir fait le a on ne peut plus faire de b.
   $\langle a\rangle tt \wedge \langle b\rangle tt \wedge [a][b]ff$

25. 1. Non, l'attaquant fait le e de Ms, le défenseur doit choisir l'un des e de Mn, et s'il choisit celui qui mène à c, l'attaquant fait t, s'il choisit celui qui mène à t, l'attaquant fait c, d'où bloquage et attaquant gagne.

2. Oui : jeu infini donc le défenseur gagne.

3. $P3$ et $P4$: quel que soit le a choisi par l'attaquant, le défenseur peut choisir n'importe quel a, et il pourra toujours répliquer à l'action suivante.

$P1$ et $P2$: selon le a choisi par l'attaquant, le défenseur chosit un a après qui il pourra faire un b (s'il y a b après celui choisi par l'attaquant) ou un c sinon.

26. 1. réflexive, symétrique évident. Seule la transitivité doit être vérifiée (car l'union de relations d'équivalences n'est pas en général une relation d'équivalence). C'est vrai,car : si R_1, R_2 sont des bisimulations, alors $R_1 \circ R_2$ est aussi une bisimulation. Si donc sR_1s_1 et $s_1R_2s_2$, alors $sR_1 \circ R_2s_2$, et s et s_2 sont aussi dans $\sim$.

2. résulte de ce que 1) $\sim$ est une bisimulation, et 2) $\sim$ contient toutes les bisimulations.

27. 2. Non. Soit $R = \{(P,Q)\ ,\ (1,3)\ ,\ (2,4)\}$. C'est une simulation, $P < Q$ et $Q < P$, mais $P \not\sim Q$: R n'est pas une bisimulation, car $P \xrightarrow{a} 0$ et il n'y a pas d'état de Q en relation avec 0 dans R (intuition).

Preuve : il ne peut pas y avoir de bisimulation entre P et Q en effet

– d'une part, comme $P \xrightarrow{a} 0$, 0 doit être bisimilaire à 3 qui est le seul état tel que $Q \xrightarrow{a} ...$

– d'autre part, comme $3 \xrightarrow{b} 4$, si 0 est bisimilaire à 3 on doit avoir une transition $0 \xrightarrow{b} ...$ qui n'existe pas : contradiction.

28. A FAIRE

29. 1. $\tau.NIL + \tau.a.NIL$ et $a.NIL$ sont-ils fortement bisimilaires ? NON.
faiblement bisimilaire ? NON $\tau.NIL + \tau.a.NIL \overset{\tau}{\Longrightarrow} NIL$ et pas $a.NIL$.
2. $a.NIL + \tau.b.NIL \overset{\tau}{\Longrightarrow} b.NIL$ et pas $a.NIL + b.NIL$ $\tau.a.NIL + \tau.b.NIL \overset{\tau}{\Longrightarrow} a.NIL$ et pas $a.NIL + \tau.b.NIL$. etc.
3. remarquer que $\Longrightarrow$ permet 0 actions.

30. Oui, la bisimulation est : $\sim = \{(0,0'), (1,1'), (2,2'), (3,3'), (4,3'), (4,4')\}$. Se vérifie facilement en regardant toutes les transitions.

31. Oui, la bisimulation est : $\sim = \{(P,Q), (P_1,Q_1), (P,Q_2), (P_1,Q_3)\}$. Se vérifie facilement en regardant toutes les transitions.

32. Soit A l'attaquant et D le défenseur.
1. Est-ce que $S \sim T$? Non. Stratégie gagnante universelle pour A : A choisit S et va en $s1$; D ne peut que aller en $t1$. A choisit $s1$ et va en $s2$, et la suite dépend de ce que fera D (qui est forcé de choisir $t1$) :

– si D reste en $t1$, A choisit $s2$ et va en S, et D perd car il ne peut pas faire de a.

– si D va en $t2$, A choisit $s2$ et reste en $s2$, et D perd car il ne peut pas faire de b.

Il y a une autre stratégie gagnante pour A.
2. $S \sim U$? Oui. Stratégie gagnante universelle pour D :

2.1 au départ de (S,U), A peut faire
- $S \xrightarrow{a} s1$, alors D fait $U \xrightarrow{a} u1$, ou bien
- $U \xrightarrow{a} u1$, alors D fait $S \xrightarrow{a} s1$.

2.2 au départ de $(s1,u1)$, A peut faire
- $s1 \xrightarrow{b} s2$, alors D fait $u1 \xrightarrow{b} u3$, ou bien
- $u1 \xrightarrow{b} u3$, alors D fait $s1 \xrightarrow{b} s2$.

2.2 au départ de $(s2,u3)$, A peut faire
- $s2 \xrightarrow{b} s2$, alors D fait $u3 \xrightarrow{b} u2$, ou bien
- $u3 \xrightarrow{b} u2$, alors D fait $s2 \xrightarrow{b} s2$, ou bien
- $s2 \xrightarrow{a} S$, alors D fait $u3 \xrightarrow{a} U$, ou bien
- $u3 \xrightarrow{a} U$, alors D fait $s2 \xrightarrow{a} S$. Dans les deux derniers cas on se retrouve à la configuration départ.

Il suffit donc d'étudier la configuration $(s2,u2)$.

2.2 au départ de $(s2,u2)$, D prendra la transition de même étiquette que celle prise par A, et donc soit on reste en $(s2,u2)$, soit on revient à la configuration départ.

Le jeu est infini et D gagne.

3. $S \sim V$? Non. Stratégie gagnante universelle pour A : A choisit S et va en $s1$; D ne peut que aller en $v1$. Ensuite, A choisit $v1$ et fait $v1 \xrightarrow{b} v2$: D doit faire $s1 \xrightarrow{b} s2$. Maintenant, A peut choisir de faire $s2 \xrightarrow{b} s2$, et D est bloqué car pas de b au départ de $v2$.