

Zagaza 1.

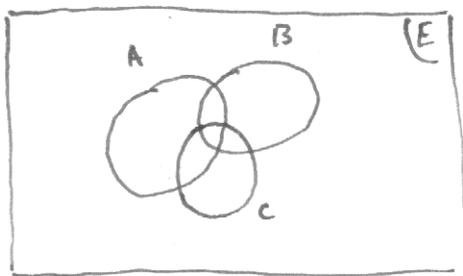
Soient A, B et C des sous-ensembles d'un ensemble E .

On veut prouver que $A \setminus (B \cup C) = (A \setminus B) \setminus C$

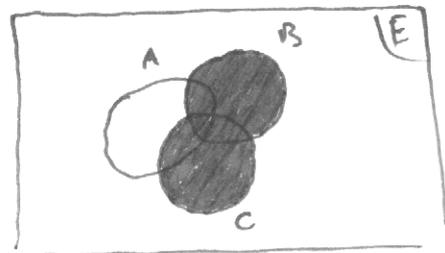
1/ Avec des diagrammes de Venn.

Déjà, je commence par faire remarquer que c'est complètement stupide, car un diagramme ne prouve rien. Mais bon, allons-y.

Supposons que la situation est la suivante :

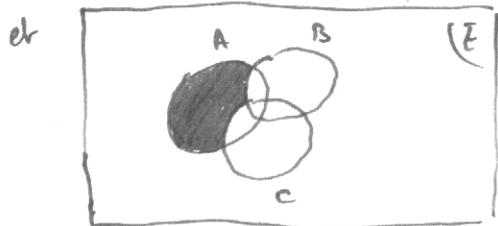


On a alors :



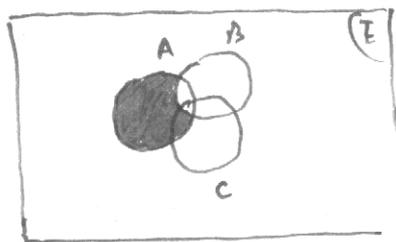
■ = $(B \cup C)$

□ = $(B \cup C)^c$

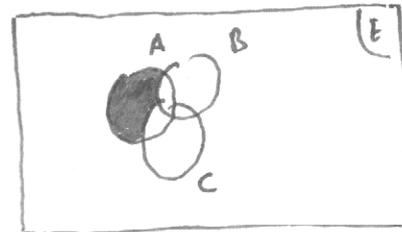


■ : $A \setminus (B \cup C)$ (qui est $A \cap (B \cup C)^c$ par définition)

D'autre part :



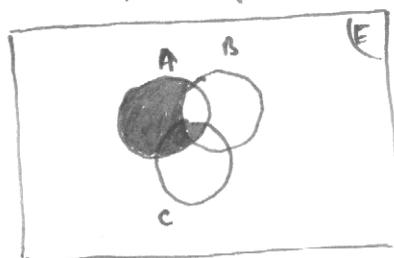
■ : $(A \setminus B)$ et
(qui est $A \cap B^c$ par définition)



■ : $(A \setminus B) \setminus C$
(qui est $(A \cap B^c) \cap C^c$ par définition)

"On voit bien sur le dessin" que $A \setminus (B \cup C) = (A \setminus B) \setminus C$.

Si j'étais le prof, je lui demanderais ensuite de dessiner $A \setminus (B \cap C)$, juste pour voir si elle a compris ce qu'elle fait. Auquel cas, on doit obtenir ça :



■ : $A \setminus (B \cap C)$

On voit bien que ce n'est pas la même chose, dans ce cas particulier, que $(A \setminus B) \setminus C$.

2/ Par un raisonnement rigoureux.

On prouve que $A \setminus (B \cup C) \subset (A \setminus B) \setminus C$ et que $(A \setminus B) \setminus C \subset A \setminus (B \cup C)$.

• Soit $x \in A \setminus (B \cup C)$.

Alors $x \in A$ et x n'est pas dans $B \cup C$. (ça veut dire que x n'est pas dans B et x n'est pas dans C .)

Donc $x \in A \setminus B$ (car $x \in A$ et $x \notin B$)

et $x \in (A \setminus B) \setminus C$ (car $x \in (A \setminus B)$ et $x \notin C$).

D'où $A \setminus (B \cup C) \subset (A \setminus B) \setminus C$.

• Réciproquement, soit $x \in (A \setminus B) \setminus C$.

Alors $x \in A \setminus B$ et $x \notin C$. La première relation dit que $x \in A$ et $x \notin B$.

Donc x est dans A , mais pas dans B ni dans C .

x est dans A , mais pas dans $B \cup C$

x est dans $A \setminus (B \cup C)$.

et $(A \setminus B) \setminus C \subset A \setminus (B \cup C)$

3/ Par le calcul

$$A \setminus (B \cup C) = A \cap (B \cup C)^c \quad (\text{définition de } \setminus).$$

$$= A \cap (B^c \cap C^c) \quad (\text{loi de De Morgan})$$

$$= (A \cap B^c) \cap C^c \quad (\text{associativité de } \cap)$$

$$= (A \setminus B) \cap C^c \quad (\text{définition de } \setminus)$$

$$= (A \setminus B) \setminus C \quad (\text{définition de } \setminus).$$

$$\underline{A \setminus (B \cup C) = (A \setminus B) \setminus C}$$

4/ Avec les fonctions caractéristiques.

Si $\Omega \subset E$, on note χ_Ω la fonction caractéristique de Ω . Par définition:

$$\forall x \in E, \chi_\Omega(x) = \begin{cases} 1 & \text{si } x \in \Omega \\ 0 & \text{si } x \notin \Omega. \end{cases}$$

On rappelle les propriétés qu'on va utiliser: si Ω_1 et Ω_2 sont deux sous-ensembles de E , alors:

$$(1) \chi_{\Omega_1 \cap \Omega_2} = \chi_{\Omega_1} \cdot \chi_{\Omega_2}$$

$$(2) \chi_{\Omega_1^c} = 1 - \chi_{\Omega_1}$$

$$(3) \chi_{\Omega_1 \cup \Omega_2} = \chi_{\Omega_1} + \chi_{\Omega_2} - \chi_{\Omega_1 \cap \Omega_2} = \chi_{\Omega_1} + \chi_{\Omega_2} - \chi_{\Omega_1} \chi_{\Omega_2}$$

On a:

$$\begin{aligned}X_{A \setminus (B \cup C)} &= X_{A \cap (B \cup C)^c} && \text{(définition de } \setminus \text{)} \\&= X_A \cdot X_{(B \cup C)^c} && \text{(propriété (1))} \\&= X_A \cdot (1 - X_{B \cup C}) && \text{(propriété (2))} \\&= X_A (1 - X_B - X_C + X_B X_C) && \text{(propriété (3))} \\&= X_A (1 - X_B) + X_A X_C (X_B - 1) && \text{(on développe)} \\&= X_A X_{B^c} - X_A X_C X_{B^c} && \text{(propriété (2))} \\&= X_A X_{B^c} (1 - X_C) && \text{(on factorise)} \\&= X_{A \cap B^c} \cdot X_{C^c} && \text{(propriétés (1) et (2))} \\&= X_{A \setminus B} \cdot X_{C^c} && \text{(définition de } \setminus \text{)} \\&= X_{(A \setminus B) \cap C^c} && \text{(propriété (1))} \\& && \text{(définition de } \setminus \text{)}.\end{aligned}$$

$$\underline{X_{A \setminus (B \cup C)}} = \underline{X_{(A \setminus B) \cap C^c}}$$

$A \setminus (B \cup C)$ et $(A \setminus B) \cap C^c$ ont la même fonction caractéristique, donc ils sont égaux. C'est vraiment passionnant.

3ogara 2.

On a un ensemble $A = \{1, 2, 3, 4, 5\}$ et deux relations ρ et τ sur A , définies par leurs graphes Γ_ρ et Γ_τ :

$$\Gamma_\rho = \{ (x, y) \in A^2 \mid |(x-2)(y-2)| \leq 1 \}$$

$$\Gamma_\tau = \{ (x, y) \in A^2 \mid 2x > 3y \} = \{ (x, y) \in A^2 \mid 3y - 2x \leq 0 \}$$

Pour chaque $(x, y) \in A^2$, on vérifie s'il est dans Γ_ρ ou Γ_τ .
Le plus simple est de faire un tableau; dans chaque case, on calcule $|(x-2)(y-2)|$ et $3y-2x$

x \ y	1	2	3	4	5
1	1 _x	0 _x	1 _x	2	3
2	0 _x				
3	1 _x	0 _x	1 _x	2	3
4	2	0 _x	2	4	6
5	3	0 _x	3	6	9

Calcul de $|(x-2)(y-2)|$.

On garde les cases où c'est inférieur à 1.

La matrice de ρ est obtenue en faisant un tableau similaire, où on met des "1" dans les bonnes cases, et des "0" dans les mauvaises:

$$\text{Mat } \rho = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

x \ y	1	2	3	4	5
1	1	4	7	10	13
2	-1 _x	2	5	8	11
3	-3 _x	0	3	6	9
4	-5 _x	-2 _x	1	4	7
5	-7 _x	-4 _x	-1 _x	2	5

Calcul de $3y-2x$.

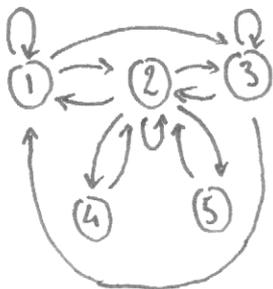
On garde les cases où le résultat est négatif.

Même chose:

$$\text{Mat } \tau = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}$$

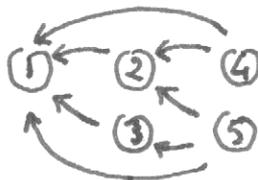
La représentation graphique de ρ est obtenue en représentant les entiers 1 à 5, et en reliant deux entiers x et y par une flèche de x vers y si $(x,y) \in T_\rho$.

On obtient :



- ρ n'est pas réflexive car $(5,5) \notin T_\rho$.
- ρ est symétrique car :
 $\forall (x,y) \in A^2, (x,y) \in T_\rho \Leftrightarrow |(x-2)(y-2)| \leq 1$
 $\Leftrightarrow |(y-2)(x-2)| \leq 1$
 $\Leftrightarrow (y,x) \in T_\rho$.
- ρ n'est pas antisymétrique, car
 $(1,2) \in T_\rho, (2,1) \in T_\rho$,
 mais $1 \neq 2$.
- ρ n'est pas transitive, car
 $(1,2) \in T_\rho, (2,5) \in T_\rho$
 mais $(1,5) \notin T_\rho$.

Même chose pour représenter τ .



- τ n'est pas réflexive car $(1,1) \notin T_\tau$
- τ n'est pas symétrique car $(2,1) \in T_\tau$
 mais $(1,2) \notin T_\tau$
- Pour l'antisymétrie, c'est un peu moins trivial. On prend $(x,y) \in A^2$ et on suppose que $(x,y) \in T_\tau$ et $(y,x) \in T_\tau$.
 Ça signifie : $3y \leq 2x$ et $3x \leq 2y$
 D'où $3y \leq 2x \leq 2 \cdot \frac{3x}{3} \leq 2 \cdot \frac{2y}{3} = \frac{4y}{3}$.
 et $3y \leq 4y$ et $y \leq 0$, ce qui est impossible.
 Donc " $(x,y) \in T_\tau$ et $(y,x) \in T_\tau$ "
 est faux et l'implication
 " $(x,y) \in T_\tau$ et $(y,x) \in T_\tau \Rightarrow x=y$ "
 est vraie. Ainsi, τ est antisymétrique.
- τ est transitive puisque si
 $(x,y) \in T_\tau$ et $(y,z) \in T_\tau$, alors :
 $3z \leq 2x$ et $3z \leq 2y$
 puis $3z \leq 2y = 2 \cdot \frac{3z}{3} \leq 2 \cdot \frac{2x}{3} = \frac{4x}{3} \leq 2x$.
 D'où $(x,z) \in T_\tau$.

Enfin, on étudie $\rho \circ \tau$. Par définition:

$$\Gamma_{\rho \circ \tau} = \{ (x, z) \in A^2 \mid \exists y \in A \quad (x, y) \in \Gamma_\tau \text{ et } (y, z) \in \Gamma_\rho \}$$

On peut essayer de tester à la main toutes les possibilités. (C'est très
dûle et intéressant. Ou bien on peut aller plus vite avec les
matrices de ρ et τ . On note $R = \text{Mat } \rho$ et $T = \text{Mat } \tau$, calculées

précédemment. Par définition,

$$\forall (x, y) \in A^2 \quad R(x, y) = \begin{cases} 1 & \text{si } (x, y) \in \Gamma_\rho \\ 0 & \text{si } (x, y) \notin \Gamma_\rho \end{cases}$$

$$T(x, y) = \begin{cases} 1 & \text{si } (x, y) \in \Gamma_\tau \\ 0 & \text{si } (x, y) \notin \Gamma_\tau \end{cases}$$

Le produit matriciel TR est défini par:

$$\forall (x, z) \in A^2 \quad (TR)(x, z) = \sum_{y \in A} \underbrace{T(x, y) R(y, z)}_{\geq 0}$$

$$\text{donc : } \forall (x, z) \in A^2 \quad \left[(TR)(x, z) = 0 \iff \begin{aligned} & (\forall y \in A \quad T(x, y) R(y, z) = 0) \\ & \iff (\forall y \in A \quad T(x, y) = 0 \text{ ou } R(y, z) = 0) \\ & \iff (\forall y \in A \quad (x, y) \notin \Gamma_\tau \text{ ou } (y, z) \notin \Gamma_\rho) \\ & \iff \text{Non } (\exists y \in A \quad (x, y) \in \Gamma_\tau \text{ et } (y, z) \in \Gamma_\rho) \\ & \iff \text{Non } ((x, z) \in \Gamma_{\rho \circ \tau}) \end{aligned} \right]$$

$$\text{et } \forall (x, y) \in A^2 \quad \left[(TR)(x, y) \neq 0 \iff (x, y) \in \Gamma_{\rho \circ \tau} \right]$$

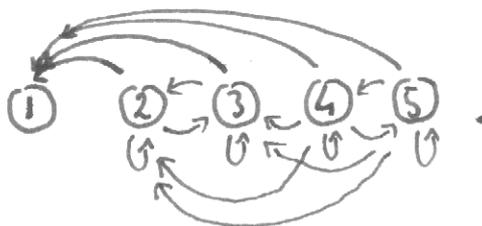
Donc on calcule TR et on cherche les coefficients non nuls:

$$TR = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 2 & 2 & 2 & 1 & 1 \\ 3 & 3 & 3 & 1 & 1 \end{bmatrix}$$

$$\text{Donc } \text{Mat } \rho \circ \tau = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

- $\rho \circ \tau$ n'est pas réflexif car $(1, 1) \notin \Gamma_{\rho \circ \tau}$
- $\rho \circ \tau$ n'est pas symétrique car $(1, 2) \notin \Gamma_{\rho \circ \tau}$
et $(2, 1) \in \Gamma_{\rho \circ \tau}$.
- $\rho \circ \tau$ n'est pas antisymétrique car $(2, 3) \in \Gamma_{\rho \circ \tau}$
et $(3, 2) \in \Gamma_{\rho \circ \tau}$
mais $3 \neq 2$.

Graphes de $\rho \circ \tau$:



• $p=7$ est la suite. Je ne vais pas de manière simple de le prouver, à part en testant toutes les possibilités:

$$\begin{array}{l} (5,5) \in \Gamma_{p=7} \quad \text{et} \quad (5,5) \in \Gamma_{p=7} \quad \text{et} \quad (5,5) \in \Gamma_{p=7} \\ (5,4) \in \Gamma_{p=7} \quad \quad \quad (5,4) \in \Gamma_{p=7} \\ (5,3) \in \Gamma_{p=7} \quad \quad \quad (5,3) \in \Gamma_{p=7} \\ (5,2) \in \Gamma_{p=7} \quad \quad \quad (5,2) \in \Gamma_{p=7} \\ (5,1) \in \Gamma_{p=7} \quad \quad \quad (5,1) \in \Gamma_{p=7} \end{array}$$

donc $\forall x \in A, ((5,5) \in \Gamma_{p=7} \text{ et } (5,x) \in \Gamma_{p=7}) \Rightarrow (5,x) \in \Gamma_{p=7}$.

$$\begin{array}{l} (5,4) \in \Gamma_{p=7} \quad \text{et} \quad (4,5) \in \Gamma_{p=7} \quad \text{et} \quad (5,5) \in \Gamma_{p=7} \\ (4,4) \in \Gamma_{p=7} \quad \quad \quad (5,4) \in \Gamma_{p=7} \\ (4,3) \in \Gamma_{p=7} \quad \quad \quad (5,3) \in \Gamma_{p=7} \\ (4,2) \in \Gamma_{p=7} \quad \quad \quad (5,2) \in \Gamma_{p=7} \\ (4,1) \in \Gamma_{p=7} \quad \quad \quad (5,1) \in \Gamma_{p=7} \end{array}$$

donc $\forall x \in A, ((5,4) \in \Gamma_{p=7} \text{ et } (4,x) \in \Gamma_{p=7}) \Rightarrow (5,x) \in \Gamma_{p=7}$.

etc...

Lagrange 3.

$p=97$ est un nombre premier donc $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$

et $|(\mathbb{Z}/p\mathbb{Z})^\times| = 96$.

On note $b=8$ et $H = \langle b \rangle$ le sous-groupe de $(\mathbb{Z}/p\mathbb{Z})^\times$ engendré par b .
On sait alors que $|H| = \min\{n \in \mathbb{N}^+ \mid b^n = 1 [97]\}$ et que
 $H = \{1, b, \dots, b^{|H|-1}\}$.

Donc pour déterminer H , il suffit de trouver $|H|$, en calculant par exemple les puissances successives de b dans $(\mathbb{Z}/p\mathbb{Z})^\times$. On calcule:

$$\begin{aligned} b &= 8 [97] & b^2 &= 64 [97] = -33 [97] & b^4 &= (-33)^2 [97] = 9 \times 121 [97] \\ & & & & &= 9 \times 24 [97] = 3 \times 72 [97] \\ & & & & &= 3 \times (-25) [97] = -75 [97] \\ & & & & & b^4 &= 22 [97] \end{aligned}$$

$$b^8 = (22)^2 [97] = 4 \times 121 [97] = 4 \times 24 [97] = 96 [97] = -1 [97].$$

$$b^{16} = 1 [97]$$

On sait alors que $|H| \mid 16$. Mais b, b^2, b^4, b^8 sont différents de $1 [97]$

donc $|H| = 16$.

Finalement, $H = \{ 1, 8, -33, 27, 22, -18, -47, 12, -1, -8, 33, -77, -22, 18, 47, \dots \}$
 $\quad \quad \quad 1 \quad b \quad b^2 \quad b^3 \quad b^4 \quad b^5 \quad b^6 \quad b^7 \quad b^8 \quad b^9 \quad b^{10} \quad b^{11} \quad b^{12} \quad b^{13} \quad b^{14} \quad b^{15}$
calculés modulo 97.

$$H = \{ \pm 1, \pm 8, \pm 12, \pm 18, \pm 22, \pm 27, \pm 33, \pm 47 \}.$$

On prend $g=9$ et on calcule gH . Il suffit de multiplier tout par 9 et de réduire modulo 97 :

$$\begin{array}{llll} 9 \times 1 = 9 \pmod{97} & 9 \times 8 = 72 = -25 \pmod{97} & 9 \times 12 = 11 \pmod{97} & 9 \times 18 = -32 \pmod{97} \\ 9 \times 22 = 4 \pmod{97} & 9 \times 27 = -48 \pmod{97} & 9 \times 33 = 6 \pmod{97} & 9 \times 47 = 35 \pmod{97}. \end{array}$$

$$gH = \{ \pm 4, \pm 6, \pm 9, \pm 11, \pm 25, \pm 32, \pm 35, \pm 48 \}.$$

Pour le reste de l'exercice, je ne comprends pas ce dont il s'agit.

3agaza 3

On a l'automate fini \mathcal{A} défini par l'alphabet $\{a, b\}$

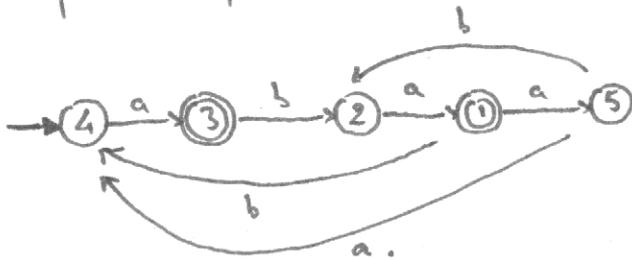
les états $\{q_1, q_2, q_3, q_4, q_5\}$

les entrées $\{q_4\}$

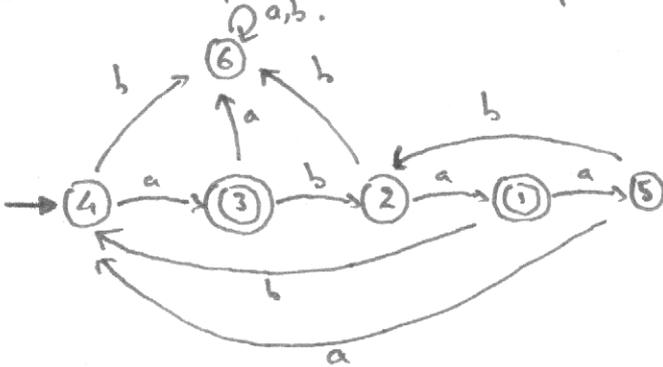
les sorties $\{q_1, q_3\}$

les transitions $\{(1, 5, a), (1, 4, b), (2, 1, a), (3, 2, b), (4, 3, a), (5, 2, b), (5, 4, a)\}$.

On peut le représenter ainsi:



Il est presque déterministe: il suffit de lui ajouter un état "poubelle" pour tenir compte des transitions qui ne sont pas définies. Voici la version déterministe:



On note, pour $i \in \{1, 2, 3, 4, 5\}$, X_i le langage reconnu si on démarre à l'état i , par l'automate \mathcal{A} . Le langage reconnu par \mathcal{A} est X_4 , puisque 4 est l'état initial.

On a successivement:

$X_4 = aX_3$ car $(4 \xrightarrow{a} 3)$ est la seule transition à partir de 4.

$X_3 = bX_2 + 1$ car $(3 \xrightarrow{b} 2)$ est la seule transition à partir de 3 et 3 accepte le mot vide.

$X_2 = aX_1$ car $(2 \xrightarrow{a} 1)$ est la seule transition à partir de 2.

$X_1 = aX_5 + bX_4 + 1$ car on a deux transitions à partir de 1: $(1 \xrightarrow{a} 5)$ et $(1 \xrightarrow{b} 4)$ et 1 accepte le mot vide.

$X_5 = aX_4 + bX_2$ car on a deux transitions à partir de 5: $(5 \xrightarrow{a} 4)$ et $(5 \xrightarrow{b} 2)$.

On résout le système et on essaie de le réécrire:

$$\begin{cases} X_1 = & bX_4 + aX_5 + 1 \\ X_2 = aX_1 \\ X_3 = & bX_2 & + 1 \\ X_4 = & aX_3 \\ X_5 = & bX_2 & + aX_4 \end{cases}$$

On commence par remplacer X_2 par aX_1 partout:

$$\begin{cases} X_1 = & bX_4 + aX_5 + 1 \\ X_2 = aX_1 \\ X_3 = baX_1 & + 1 \\ X_4 = & aX_3 \\ X_5 = baX_1 & + aX_4 \end{cases}$$

Puis on remplace X_3 par $baX_1 + 1$ partout:

$$\begin{cases} X_1 = & bX_4 + aX_5 + 1 \\ X_2 = aX_1 \\ X_3 = baX_1 & + 1 \\ X_4 = abaX_1 & + a \\ X_5 = baX_1 & + aX_4 \end{cases}$$

Puis on remplace X_4 par $abaX_1 + a$:

$$\begin{cases} X_1 = babaX_1 & + aX_5 + ba + 1. \\ X_2 = aX_1 \\ X_3 = baX_1 \\ X_4 = abaX_1 & + a \\ X_5 = (ba + a^2ba)X_1 & + a^2 \end{cases}$$

Enfin, on remplace X_5 par $(ba + a^2ba)X_1 + a^2$:

$$\begin{cases} X_1 = (baba + aba + a^3ba)X_1 & + a^2 + ba + 1. \\ X_2 = aX_1 \\ X_3 = baX_1 \\ X_4 = abaX_1 & + a \\ X_5 = (ba + a^2ba)X_1 & + a^2 \end{cases}$$

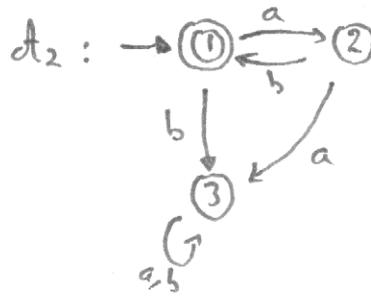
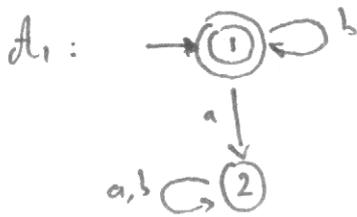
On sait alors (théorème du cours) que: $X_1 = (baba + aba + a^3ba)^* (a^2 + ba + 1)$

d'où $X_4 = abaX_1 = aba (baba + aba + a^3ba)^* (a^2 + ba + 1)$

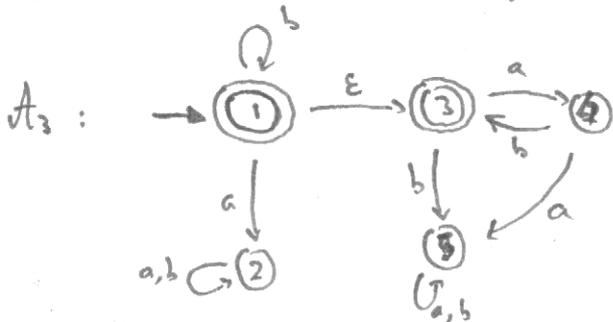
Le langage reconnu par A est $L = aba (baba + aba + a^3ba)^* (a^2 + ba + 1)$

On peut vérifier, à titre d'exemple, que $aba^4ba^2ba = aba \cdot a^3ba \cdot aba$ est accepté,
et que ba^3 est refusé.

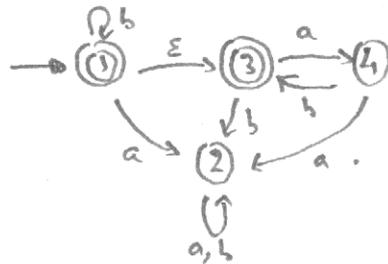
On note $L_0 = \{ a b^n (ab)^m \mid m, n \in \mathbb{N} \}$ et on cherche un automate qui reconnait L_0 .
 On remarque que $L_0 = a L_1 L_2$ avec $L_1 = \{ b^n \mid n \in \mathbb{N} \}$ et $L_2 = \{ (ab)^m \mid m \in \mathbb{N} \}$.
 Construire des automates qui acceptent L_1 et L_2 est évident;



On obtient un automate acceptant $L_1 L_2$ en reliant A_1 et A_2 par une ϵ -transition entre l'état final de A_1 et l'état initial de A_2 :



Mais on préfère avoir une version déterministe de cet automate. On commence par remarquer que 2 et 5 sont des états "poubelle", donc A_3 est équivalent à A_4 :



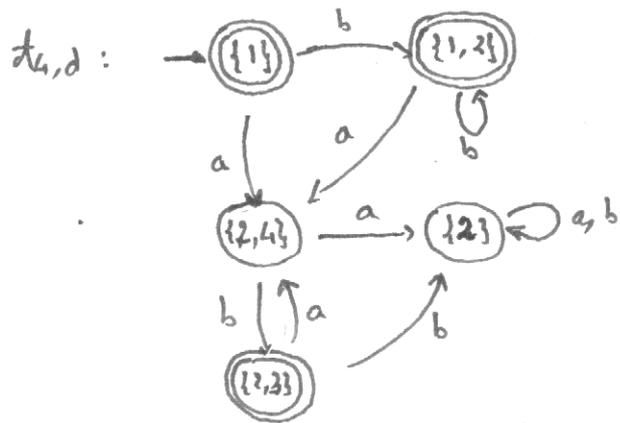
Il reste à supprimer l' ϵ -transition. On utilise la méthode (probablement étudiée en cours):

Etat	a	b
{1}	{2,4}	{1,2}
{2,4}	{2}	{2,3}
{2}	{2}	{2}
{2,3}	{2,4}	{2}
{1,2}	{2,4}	{1,2}

car à partir de 1, avec un a, on peut aller en 2 ou en 4 (avec ϵ -transition par 3)
 avec un b, on peut aller en 1 ou en 2 (avec ϵ -transition par 3).

Même raisonnement.

D'où une version déterministe de $A_{4,d}$:



$A_{4,d}$ reconnaît $L_1, L_2 = \{ b^n (ab)^m \mid m, n \in \mathbb{N} \}$. Pour reconnaître $L_0 = aL_1L_2$, il suffit de laisser passer un a et d'envoyer b à la portelle $\{2\}$ si le mot commence par b . Ceci nous donne un automate A_0 qui reconnaît L_0 :

