Mathématiques discrètes
Semestre 1 – LU2IN005

Anja JANKOVIC – Faculté des Sciences et Ingénierie
13 septembre au 14 décembre 2022

Table des matières

Thaïs MILLERET – Mono Informatique G4

TD 1 : Ensembles, relations, fonctions

Exercice 1. Ensembles

1. Calculer $S_1 \times S_1$ pour $S_1 = \{0, 1, 2\}$.

$$S_1 \times S_1 = \{(0{,}0), (0{,}1), (0{,}2),\\ (1{,}0), (1{,}1), (1{,}2),\\ (2{,}0), (2{,}1), (2{,}2),$$

$\mathrm{card}(S_1 \times S_1) = 3^2 = 9$

2. Calculer l'ensemble $\mathcal{P}(S)$ des parties de S pour $S = S_1$ puis pour $S = S_2 = \{1, \{1{,}4\}\}$ et enfin pour $S = S_3 = \mathcal{P}(\{1\})$.

- $S = S_1 \rightarrow \mathcal{P}(S) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0{,}1\}, \{0{,}2\}, \{1{,}2\}, S_1\}$
  $|\mathcal{P}(S)| = 8$
- $S = S_2 = \{1, \{1{,}4\}\}$ 2 éléments
  $\mathcal{P}(S) = \{\emptyset, S_2, \{1\}, \{\{1{,}4\}\}\}$ 4 éléments
- $S = S_3 = \mathcal{P}(\{1\})$
  $\rightarrow \mathcal{P}(S) = \mathcal{P}\underbrace{(\{\emptyset, \{1\}\})}_{\text{2 éléments}} = \underbrace{\{\emptyset, \{\emptyset, \{1\}\}, \{\emptyset\}, \{\{1\}\}\}}_{\text{4 éléments}}$

3. Donner toutes les partitions possibles de l'ensemble $\{1, 2, 3\}$.

Partition 1 : $S_1 = \{1\}$, $S_2 = \{2\}$, $S_3 = \{3\}$

Partition 2 : $S_1 = \{1\}$, $S_2 = \{2, 3\}$

Partition 3 : $S_1 = \{2\}$, $S_2 = \{1, 3\}$

Partition 4 : $S_1 = \{3\}$, $S_2 = \{1, 2\}$

Partition 5 : $S_1 = \{1, 2, 3\}$

Exercice 2. Raisonnement sur les ensembles

1. Soient A et B deux parties de E. Montrer que $A \cap \overline{A \cap B} = A \cap \bar{B}$.

cf. formules p.8 du Cours 1

Loi de De Morgan : $\overline{A \cap B} = \bar{A} \cup \bar{B}$

$\Rightarrow \underbrace{A \cap (\bar{A} \cup \bar{B})}_{\downarrow} = \underbrace{(A \cap \bar{A})}_{\emptyset} \cup (A \cap \bar{B}) = A \cap \bar{B}$ <u>CQFD</u>

distributivité de ∪ sur ∩

2. Soient A, B, C trois parties de E. Montrer que si $A \cap B = A \cap C$ alors $A \cap \bar{B} = A \cap \bar{C}$.

$\left.\begin{array}{l}\textbf{si } A \cap B = A \cap C \\ \textbf{alors } A \cap \bar{B} = A \cap \bar{C}\end{array}\right\}$ implication $(\Rightarrow)$

Supposons que $A \cap B = A \cap C$.

Alors, $\overline{A \cap B} = \overline{A \cap C}$ (si 2 ensembles sont égaux, alors leurs complémentaires sont égaux aussi)

Donc $\underbrace{A \cap \overline{A \cap B}}_{*} = \underbrace{A \cap \overline{A \cap C}}_{*}$ (on peut appliquer la même « opération » à gauche et à droite)

Donc $A \cap \bar{B} = A \cap \bar{C}$ <u>CQFD</u>

$*$ D'après la question 1, $A \cap \overline{A \cap B} = A \cap \bar{B}$.

3. En déduire que $A \cap \bar{B} = A \cap \bar{C}$ si et seulement si $A \cap B = A \cap C$.

$A \cap \bar{B} = A \cap \bar{C}$ $\underbrace{\text{ssi}}_{\downarrow}$ $A \cap B = A \cap C$

équivalence

Ici : (si) $A \cap \bar{B} = A \cap \bar{C} \Rightarrow A \cap B = A \cap C$ (alors)

(implication dans le sens inverse)

Supposons que $A \cap \underbrace{\bar{B}}_{X} = A \cap \underbrace{\bar{C}}_{Y}$.

D'après la question 2, $A \cap \bar{X} = A \cap \bar{Y}$

$\Leftrightarrow A \cap \bar{\bar{B}} = A \cap \bar{\bar{C}}$

$\Leftrightarrow A \cap B = A \cap C$ <u>CQFD</u>

En montrant 2 implications, on a montré l'équivalence.

4. Soient A, B, C trois parties de E. Montrer que si ($A \cup B \subseteq A \cup C$ et $A \cap B \subseteq A \cap C$) alors $B \subseteq C$. Dans quel cas a-t-on l'égalité $B = C$?

si … alors : implication $\Rightarrow$

Supposons que $A \cup B \subseteq A \cup C$ et $A \cap B \subseteq A \cap C$.

$A \cup B \subseteq A \cup C$ et $B \subseteq A \cup B$[1] donc par transitivité de $\subseteq$ on a $\boldsymbol{B} \subseteq \boldsymbol{A} \cup \boldsymbol{C}$ et par conséquent $\boldsymbol{B} \subseteq \boldsymbol{B} \cap (\boldsymbol{A} \cup \boldsymbol{C})$[2].

Par distributivité de $\cap$ sur $\cup$: $B \subseteq (A \cap B) \cup (B \cap C) \subseteq (A \cap C) \cup (B \cap C)$

Donc $B \subseteq (A \cap C) \cup (B \cap C)$.

Par distributivité de $\cup$ sur $\cap$, on regroupe les termes.

Donc $\underbrace{B \subseteq (A \cup B)}_{\text{direct}} \cap C$ $\rightarrow$ par intersection, $B \subseteq (A \cup B)$ et $B \subseteq C$

Donc $\boldsymbol{B} \subseteq \boldsymbol{C}$ <u>CQFD</u>

Pour avoir l'égalité $B = C$, on doit avoir $\underbrace{B \subseteq C}_{1}$ et $\underbrace{C \subseteq B}_{2}$.

1) $A \cup B \subseteq A \cup C$ et $A \cap B \subseteq A \cap C$
2) $A \cup C \subseteq A \cup B$ et $A \cap C \subseteq A \cap B$

$B = C$ <u>ssi</u> $A \cup B = A \cup C$ et $A \cap B = A \cap C$

[1] Un ensemble B est inclus dans l'union de lui-même avec un autre ensemble.

[2] Si B est inclus dans un ensemble, alors il est aussi inclus dans sa propre intersection avec cette ensemble.

5. Montrer que $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

On utilise les définitions du produit cartésien et de l'intersection.

$$\begin{aligned} A \times (B \cap C) &= \{(x,y) \mid x \in A \text{ et } y \in B \cap C\} \quad \text{définition du produit cartésien} \\ &= \{(x,y) \mid x \in A, y \in B, y \in C\} \quad \text{définition de l'intersection} \\ &= \{(x,y) \mid (x,y) \in A \times B \text{ et } (x,y) \in A \times C\} \\ &= \{(x,y) \mid (x,y) \in (A \times B) \cap (A \times C)\} \\ &= (A \times B) \cap (A \times C) \end{aligned}$$

6. A-t-on (1) $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$? OUI (2) $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$? NON

(1) On a (1) puisque :

$E \in \mathcal{P}(A \cap B)$
$\Leftrightarrow E \subseteq A \cap B$
$\Leftrightarrow E \subseteq A$ et $E \subseteq B$
$\Leftrightarrow E \in \mathcal{P}(A)$ et $E \in \mathcal{P}(B)$
$\Leftrightarrow E \in \mathcal{P}(A) \cap \mathcal{P}(B)$

Attention à la différence entre $\in$ et $\subseteq$:

Dans $E \in \mathcal{P}(A \cap B)$, on regarde E comme un élément de l'ensemble des parties.

Dans $E \subseteq A \cap B$, on regarde E comme un sous-ensemble de $A \cap B$.

(2) Contre-exemple :

$A = \{1,2,3\}$ $B = \{4,5\}$ On a $\{3,5\} \in \mathcal{P}(A \cup B)$ mais $\{3,5\} \notin \mathcal{P}(A) \cup \mathcal{P}(B)$.

Autre façon : remarquer que $|A \cup B| = |A| + |B| - |A \cap B|$

7. Soit E un sous-ensemble d'un ensemble F et x un élément de F qui n'appartient pas à E. Montrer que $\mathcal{P}(E \cup \{x\}) = \mathcal{P}(E) \cup \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$.

On nous demande de prouver que l'ensemble des parties de $E \cup \{x\}$ (ensemble E plus un point x qui n'appartient pas à E) est égal à l'ensemble des parties de E plus l'ensemble formé en prenant chaque partie de $\mathcal{P}(E)$ à laquelle on ajoute x.

On montre 2 inclusions :

$\subseteq$: $\mathcal{P}(E \cup \{x\}) \subseteq \mathcal{P}(E) \cup \big\{\{x\} \cup A \bigm| A \in \mathcal{P}(E)\big\}$

Soit $B \in \mathcal{P}(E \cup \{x\})$.

1) Si $x \in B$: alors $B \backslash \{x\}$ est une partie de E et donc $B \in \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$. Par conséquent, $B \in \mathcal{P}(E) \cup \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$.
2) Si $x \notin B$: alors B est une partie de E donc $B \in \mathcal{P}(E)$ donc $B \in \mathcal{P}(E) \cup \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$.

On différencie deux cas. Soit B contient x et $B \in \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$. Soit B ne contient pas x et $B \in \mathcal{P}(E)$. Dans les deux cas, B appartient à l'union.

$\supseteq$: $\mathcal{P}(E) \cup \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\} \subseteq \mathcal{P}(E \cup \{x\})$

Soit $B \in \mathcal{P}(E) \cup \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$.

Donc $B \in \mathcal{P}(E)$ ou $B \in \big\{\{x\} \cup A \mid A \in \mathcal{P}(E)\big\}$.

D'où $B \subseteq E$ ou $B = \{x\} \cup$ pour $\underbrace{A}_{A \subseteq E}$ une partie de E quelqconque

Donc $B \subseteq E \cup \{x\}$

et finalement $B \in \mathcal{P}(E \cup \{x\})$.

Remarque : Cette démonstration est une étape de la démonstration par récurrence qui permet de démontrer que le cardinal de $\mathcal{P}(E)$ est 2^n avec n le cardinal de E.

E de cardinal $n = 0 \Rightarrow \mathcal{P}(E) = \{\emptyset\}$, card $= 2^n = 2^0 = 1$ E de cardinal n (quelconque) $\Rightarrow E \cup \{x\}$ est de cardinal $n+1$, $\text{card}(E) = 2^n$ et $\text{card}(E \cup \{x\}) = 2 \times 2^n = 2^{n+1}$

Exercice 4. Propriétés de base des relations binaires

1. On considère la relation $R = \{(1,1), (2,3), (3,2)\}$ définie sur $E = \{1, 2, 3\}$. Déterminer si R est réflexive, symétrique, antisymétrique, transitive.

réflexive : $(3,3) \notin R$ non

symétrique : oui (car 1 en relation avec 1, 2 en relation avec 3 et inversement)

antisymétrique : $(2,3)$ et $(3,2)$ mais $2 \neq 3$ non

transitive : non

2. La relation R définie sur $\mathbb{N}$ par $(n, m) \in \mathbb{R}$ si et seulement si n et m ont un diviseur commun différent de 1 est-elle transitive ?

transitive : non contre-exemple :

$(2,6) \in R$ car 2 divise 2 et 6

$(3,6) \in R$ car 3 divise 2 et 6

mais $(2,3) \notin R$ car 1 est le seul diviseur commun de 2 et 3

3. On définit la relation R sur l'ensemble $\mathcal{P}(E)$ des parties de E par $(x, y) \in R$ si et seulement si $x \cap y \neq \emptyset$. La relation R est-elle réflexive, symétrique, transitive ?

réflexive : si $x = \emptyset$, alors $(x, x) = (\emptyset, \emptyset)$ et $\emptyset \cap \emptyset = \emptyset$ donc non

symétrique : oui car si $x \cap y \neq \emptyset$, alors $y \cap x \neq \emptyset$.

transitive : si $x \cap y \neq \emptyset$ et $y \cap z \neq \emptyset$, alors $x \cap z \neq \emptyset$ non

contre-exemple : $E = \{1, 2, 3, 4\}$ $x = \{1, 2\}$ $y = \{2, 3\}$ $z = \{3, 4\}$

2 appartient à x et y et 3 appartient à y et z, mais il n'y a pas d'éléments communs à x et z.

Rappel

Relation d'ordre : réflexive, antisymétrique, transitive	Relation d'équivalence : réflexive, symétrique, transitive	Relation totale : $\nexists$ élément « non-couvert » par la relation

4. La relation $\preccurlyeq$, définie sur $\{0,1\} \times \{0,1\}$ par $(x_1, x_2) \preccurlyeq (y_1, y_2)$ si et seulement si $x_1 \leq y_1$ et $x_2 \leq y_2$, est-elle une relation d'ordre ? est-elle totale ?

$\{0,1\} \times \{0,1\} = \{(0,0), (0,1), (1,0), (1,1)\}$

Relation d'ordre ? oui

réflexive : oui, $(x_1, x_2) \preccurlyeq (x_1, x_2)$ ssi $x_1 \leq x_1$ et $x_2 \leq x_2$ ($\leq$ signifie que peuvent être égaux)

antisymétrique : oui, $\left.\begin{array}{c} (x_1, x_2) \preccurlyeq (y_1, y_2) \rightarrow x_1 \leq y_1 \text{ et } x_2 \leq y_2 \\ \text{et} \\ (y_1, y_2) \preccurlyeq (x_1, x_2) \rightarrow y_1 \leq x_1 \text{ et } y_2 \leq x_2 \end{array}\right\} \begin{array}{c} x_1 = y_1 \\ \text{et} \\ x_2 = y_2 \end{array}$

transitive : oui, $(x_1, x_2) \preccurlyeq (y_1, y_2)$ et $(y_1, y_2) \preccurlyeq (z_1, z_2)$

$\Leftrightarrow (x_1 \leq y_1$ et $x_2 \leq y_2)$ et $(y_1 \leq z_1$ et $y_2 \leq z_2)$

$\Leftrightarrow x_1 \leq z_1$ et $x_2 \leq z_2$

$\Leftrightarrow (x_1, x_2) \preccurlyeq (z_1, z_2)$

Donc c'est une relation d'ordre.

Totale ? non car $(0,1)$ et $(1,0)$ ne sont pas comparables

(impossible de les mettre en relation $\preccurlyeq$)

5. On définit une relation R, permettant d'exprimer que deux nombres réels $x_1, x_2 \in \mathbb{R}$ sont « équivalents » à ε près, par $(x_1, x_2) \in \mathbb{R}$ si et seulement si $|x_1 - x_2| \leq \varepsilon$. La relation R est-elle une relation d'équivalence ?

définition de ε : $\varepsilon \geq 0$

réflexive : $(x, x) \in \mathbb{R} \Leftrightarrow \underbrace{|x - x|}_{=0} \leq \varepsilon$ oui

symétrique : si $(x, y) \in \mathbb{R}$ alors $(y, x) \in \mathbb{R} \Leftrightarrow |x - y| \leq \varepsilon$ alors $|y - x| \leq \varepsilon$

et $|x - y| = |y - x|$ donc oui

Il y a une valeur absolue donc $|x - y| = |y - x|$.

transitive : si $(x, y) \in \mathbb{R}$ et $(y, z) \in \mathbb{R}$, alors $(x, z) \in \mathbb{R}$

$\Leftrightarrow |x - y| \leq \varepsilon$ et $|y - z| \leq \varepsilon$, alors $|x - z| \leq \varepsilon$ non

contre-exemple : $x = 1 \quad y = 2 \quad z = 3 \quad \varepsilon = 1$

$|1 - 2| \leq 1 \quad |2 - 3| \leq 1 \quad \underbrace{|1 - 3|}_{2} \nleq 1$

On aurait pu aller plus vite car le contre-exemple montrant que la relation n'est pas transitive suffit à montrer que la relation n'est pas une relation d'équivalence.

Exercice 5. Produit / Composition et inverse de relations

Rappel : Composition

$$\left.\begin{matrix} R_1 \subseteq E \times F \\ \text{et} \\ R_2 \subseteq F \times G \end{matrix}\right\} R_1 . R_2 \in E \times G$$

1. Soient $A = \{1, 2, 3, 4\}$, $B = \{1, 3, 5\}$ et $R \subseteq A \times B$ la relation définie par $(a, b) \in \mathbb{R}$ ssi $a < b$.
   (a) Écrire la relation R comme un ensemble de paires ordonnées.
   (b) Calculer les relations $R^{-1}.R$ et $R.R^{-1}$.

(a) $R = \{(1,3), (1,5), (2,3), (2,5), (3,5), (4,5)\}$

Rappel : Inverse

$(x, y) \in R^{-1}$ ssi $(x, y) \in \mathbb{R}$

Exemple : On a la relation $x < y$. La relation inverse est $y > x$. C'est une autre perspective pour regarder la même chose.

(b) $R^{-1} = \{(3, 1), (5, 1), (3, 2), (5, 2), (5,3), (5,4)\}$

R^{-1} est défini dans $B \times A$.

$R^{-1}.R \subseteq B \times B = \{(3,3), (5,3), (5,5), (3,5)\}$

$$R.R^{-1} \subseteq A \times A = \{(1,1), (1,2), (1,3), (1,4), \\ (2,1), (2,3), (2,3), (2,4), \\ (3,1), (3,2), (3,3), (3,4), \\ (4,1), (4,2), (4,3), (4,4)\}$$

On remarque que $R.R^{-1} = A \times A$.

2. Montre que pour deux relations quelconques $R \subseteq X \times Y$ et $S \subseteq Y \times Z$, on a l'égalité $(R.S)^{-1} = S^{-1}.R^{-1}$.

Par définition de l'inverse :

$(R.S)^{-1} = \{(z, x) \mid (x, z) \in R.S\}$

Par définition de la composition :

$(R.S)^{-1} = \{(z, x) \mid \exists (y \in Y | (x, y) \in R \text{ et } (y, z) \in S)\}$

$(R.S)^{-1} = \{(z, x) \mid \exists (y \in Y | (y, x) \in R^{-1} \text{ et } (z, y) \in S^{-1})\}$

$(R.S)^{-1} = S^{-1}.R^{-1}$

3. On considère la relation $R \subseteq \mathbb{N} \times \mathbb{N}$ définie par $(x, y) \in R$ si et seulement si $y = 2x$. Quels sont les éléments de R^+ ?

Rappel : Fermeture transitive R^+

Fermeture transitive = $R \cup (R.R) \cup (R.R.R) \cup \cdots$

$$= \bigcup_{i \geq 1} R^i$$

$R^1 = R = \{(x,y) \mid y = \mathbf{2^1}x\}$
$R^2 = R.R^1 = \{(x,y) \mid \exists z \mid (x,z) \in R \text{ et } (z,y) \in R\}$
$= \{(x,y) \mid z = 2x \text{ et } y = 2z\}$
$= \{(x,y) \mid y = \mathbf{2^2}x\}$
$R^3 = R.R^2 = \{(x,y) \mid \exists z \mid (x,z) \in R \text{ et } (z,y) \in R^2\}$
$= \{(x,y) \mid z = 2x \text{ et } y = 4z\}$
$= \{(x,y) \mid y = 8x = \mathbf{2^3}x\}$

On remarque que :

$R^+ = \{(x,y) \mid y = 2^n x\}$, n quelconque

Exercice 6. Composition et implications ensemblistes des propriétés des relations

Soit R une relation sur E. Montrer que :

1. R est réflexive si et seulement si $\mathrm{Id}_E \subseteq R$.

Par définition d'une relation réflexive, $\underbrace{\forall x \in E, (x,x) \in R}_{\text{définition de la relation identité}}$ et donc

$\mathrm{Id}_E \subseteq R$ (pour tout élément de E, la relation Id_E est incluse dans R).

2. R est symétrique si et seulement si $R = R^{-1}$.

2 implications $\Rightarrow$ et $\Leftarrow$

$\Rightarrow$: Supposons que R est symétrique.

Par définition d'une relation symétrique, $\forall x, y \in E$, si $(x,y) \in R$, alors $(y,x) \in R$.

Par définition de l'inverse, $\forall a, b \in E$, $(a,b) \in R$, $(b,a) \in R^{-1}$.

Si $(x,y) \in R$, alors $(x,y) \in R^{-1}$.

Donc $R \subseteq R^{-1}$.

Par identité, $\forall (x,y) \in R^{-1}$, $(y,x) \in R$.

Par symétrie, si $(y,x) \in R$, alors $(x,y) \in R$.

Donc $R^{-1} \subseteq R$.

Double inclusion $\Rightarrow R = R^{-1}$

$\Leftarrow$: Supposons que $R = R^{-1}$.

Soit $(x,y) \in R$, montrer que $(y,x) \in R$.

Par hypothèse, on a $(x,y) \in R^{-1}$.

Par définition de l'inverse, $(y,x) \in R$.

3. R est anti-symétrique si et seulement si $R \cap R^{-1} \subseteq \mathrm{Id}_E$.

2 implications $\Rightarrow$ et $\Leftarrow$

$\Rightarrow$: Supposons que R est anti-symétrique.

Par définition de l'anti-symétrie, si $(x,y) \in R$ et $(y,x) \in R$, alors $x = y$.

Si $(x,y) \in R \cap R^{-1}$, alors $(x,y) \in R$ et $(x,y) \in R^{-1}$.

Par définition de l'inverse, $(x, y) \in R^{-1} \rightarrow (y, x) \in R$.
Puisque R est anti-symétrique, on obtient $x = y$ et donc $\underbrace{(x, y)}_{x=y} \in \mathrm{Id}_E$.

Donc $R \cap R^{-1} \subseteq \mathrm{Id}_E$.

$\Leftarrow$: Supposons que $R \cap R^{-1} \subseteq \mathrm{Id}_E$.
Par définition de l'inverse, si $(x, y) \in R$ et $(y, x) \in R$, alors $(y, x) \in R^{-1}$ et $(x, y) \in R^{-1}$.
Donc $(x, y) \in R \cap R^{-1}$ et $(y, x) \in R \cap R^{-1}$.
Par hypothèse, comme $(x, y) \in \mathrm{Id}_E$ et $(y, x) \in \mathrm{Id}_E$, on retrouve $x = y$.
Donc on retrouve aussi la définition de l'anti-symétrie.

4. R est transitive si et seulement si $R.R \subseteq R$.

$\Rightarrow$: Supposons que R est transitive.
Si $(x, y) \in R.R$, alors (par définition de la composition) $\exists z$ tel que $(x, z) \in R$ et $(z, y) \in R$.
Par transitivité, on obtient $(x, y) \in R$.
On a prouvé que qu'un élément quelconque (x, y) de $R.R$ appartient aussi à R.
Donc $R.R \subseteq R$.

$\Leftarrow$: Supposons que $R.R \subseteq R$.
si $(x, y) \in R$ et $(y, z) \in R$, alors $(x, z) \in R.R$ (par définition de la composition)
Par hypothèse, $(x, y) \in R$, ce qui nous permet de retrouver la définition de la transitivité.

5. Si R est réflexive, alors $R \subseteq R.R$ et $R.R$ est aussi réflexive.

Par définition d'une relation réflexive, $\forall x \in E, (x, x) \in R$.
Par définition de la composition, si $(x, y) \in R.R$, alors $\exists z$ tel que $(x, z) \in R$ et $(z, y) \in R$.
Comme R est réflexive, $\forall x, y \in E$, il existe $(x, y) \in R.R$ et z tel que $(x, z) \in R$ et $(z, y) \in R$ avec $x = z = y$. Donc, $\forall x \in E$, si $(x, x) \in R$ alors $(x, x) \in R.R$ et $R.R$ est aussi réflexive.

6. Si R est symétrique, alors $R^{-1}.R = R^{-1}.R$.

D'après la question 2, R est symétrique si et seulement si $R = R^{-1}$. Donc $R^{-1}.R = R^{-1}.R$.

7. Si R est transitive, alors $R.R$ est transitive.

D'après la question 4, R est transitive si et seulement si $R.R \subseteq R$.
Donc, si $(x, y), (y, z) \in R.R$ alors $(x, y), (y, z) \in R$. Donc $(x, z) \in R.R$. C'est la définition de la transitivité donc $R.R$ est transitive.

Exercice 8. Partition engendrée par une relation d'équivalence

Rappel : définition (simplifiée) de la classe d'équivalence

$$\boxed{[x] = \{x' \text{ tel que } (x, x') \in R\}}$$

Soit R une relation d'équivalence dans A et soit $[a]$ la classe d'équivalence de $a \in A$.
Montrer que :

1. pour chaque $a \in A$, $a \in [A]$

Comme R est réflexive, $(a, a) \in R, \forall a \in A$, et donc $a \in [a]$.

2. $[a] = [b]$ si et seulement si $(a, b) \in R$

$\Leftarrow$: Supposons que $(a, b) \in R$.

On veut montrer que $[a] = [b]$.

On prend un élément quelconque $x \in [b]$, et on remarque que $(b, x) \in R$.

Par hypothèse, $(a, b) \in R$, donc par transitivité, $(a, x) \in R$.

En conséquence, $x \in [a]$, et donc $[b] \subseteq [a]$.

On montre que $[a] \subseteq [b]$.

Par symétrie de R, si $(a, b) \in R$, alors $(b, a) \in R$.

Donc si on inverse l'ordre de a et b, on peut appliquer le même raisonnement que pour $[b] \subseteq [a]$.

Donc $[a] \subseteq [b]$ et par conséquence $[\boldsymbol{a}] = [\boldsymbol{b}]$.

$\Rightarrow$: Supposons que $[a] = [b]$.

Les éléments de $[a]$ étant égaux aux éléments de $[b]$, on retrouve a et b dans une même classe d'équivalence, et par définition, $(a, b) \in R$.

3. si $[a] \neq [b]$ alors $[a]$ et $[b]$ sont disjointes

disjointes : $[a] \cap [b] = \emptyset$

Le plus simple est de démontrer par contraposée.

<u>Contraposée :</u> si $[a] \cap [b] \neq \emptyset$, alors $[a] = [b]$

Comme $[a] \cap [b] \neq \emptyset$, alors il existe un élément $x \in A$ tel que $x \in [a] \cap [b]$.

D'où $(a, x) \in R$ et $(b, x) \in R$. (par définition d'une classe d'équivalence)

Par symétrie de R, on a $(x, a) \in R$ et $(x, b) \in R$

et par transitivité, on a $(a, b) \in R$.

Par la question 2, on conclut que $[a] = [b]$.

4. l'ensemble des classes d'équivalence forme une partition de A

L'ensemble des classes d'équivalence forme une partition de A.

Ceci résulte des questions précédentes.

$$\begin{cases} \forall a \in A, a \in [a] \\ [a] = [b] \Leftrightarrow (a, b) \in R \\ [a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset \end{cases}$$

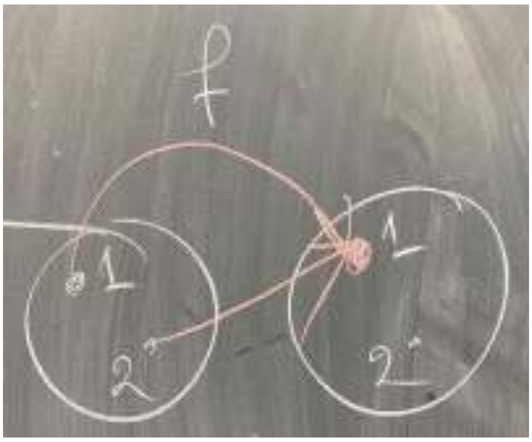
Exercice 9. Applications injectives, surjectives, bijectives : exemples

1. Trouver un exemple d'application qui n'est ni injective, ni surjective.

Rappel : fonctions

injective : au plus 1 antécédent
$\forall e_1, e_2 \in E$, si $f(e_1) = f(e_2)$ alors $e_1 = e_2$
surjective : au moins 1 antécédent
$\forall e_2 \in F, \exists e_1 \in E$ tel que $f(e_1) = e_2$
bijective : exactement 1 antécédent

schéma →



$f : \{1,2\} \to \{1,2\}$, $f(1) = f(2) = 1$ n'est ni injective, ni surjective.

2. Les applications suivantes sont-elles injectives ? sont-elles surjectives ? sont-elles bijectives ?

(a) $f_1 : \mathbb{N} \to \mathbb{N}$ telle que $f_1(x) = 3x + 1$ et $f_2 : \mathbb{Q} \to \mathbb{Q}$ telle que $f_2(x) = 3x + 1$

injective ?

$3x_1 + 1 = 3x_2 + 1$

$\Leftrightarrow 3(x_1 - x_2) = 1 - 1$

$\Leftrightarrow x_1 - x_2 = 0$

$\Leftrightarrow x_1 = x_2$

<u>f_1 et f_2 oui</u>

bijective ?

$$\forall y \in \mathbb{N}/\mathbb{Q}, \exists x = \frac{y-1}{3} \in \mathbb{N}/\mathbb{Q} \text{ ?}$$

oui pour $\mathbb{Q}$

$$x = \frac{5-1}{3} = \frac{4}{3} \notin \mathbb{N}$$

5 n'a pas d'antécédent dans $\mathbb{N}$ pour f_1.

<u>f_1 non, f_2 oui</u>

bijective ? <u>f_1 non, f_2 oui</u>

(b) $f : \mathbb{N} \to \{0, 1, 2\}$ telle que $f(x) = x \bmod 3$

injective ? <u>non</u>

car on peut prendre x_1, x_2 différents et arriver à $f(x_1) = f(x_2)$

Par exemple, $x_1 = 3$ et $x_2 = 6$, $x_1 \neq x_2$, $3 \bmod 3 = 6 \bmod 3 = 0$

Plusieurs dividendes ont le même reste par la division euclidienne par 3.

surjective ? <u>oui</u>

car pour tout $x \in \mathbb{N}$, $f(x) \in \{0, 1, 2\}$ et pour tout $p \in \{0, 1, 2\}$, on a $f(p) = p$

Tous les nombres ont un modulo.

bijective ? non

(c) $f : \mathbb{N}^2 \to \mathbb{N}$ telle que $f(x, y) = x + y$

injective ? non, car $f(0,1) = f(1,0) = 1$, $x = 0 \neq x = 1$, $y = 1 \neq y = 0$

surjective ? oui, car tout entier peut s'écrire sous la forme $x + 0 = f(x, 0)$

bijective ? non

(d) $f : \mathbb{N} \to \mathbb{N}$ telle que $f(n) = n + 1$ si n est pair et $f(n) = n - 1$ si n est impair

surjective ?

Soit $n \in \mathbb{N}$.

On distingue 2 cas : en fonction de la parité de n.

1) Si n est impair, $n - 1$ est pair et $f\underbrace{(n-1)}_{\text{pair}} = (n-1) + 1 = n$

2) Si n est pair, $n + 1$ est impair et $f(n + 1) = n$ (même raisonnement que le cas 1)

On a montré que tout n à un antécédent par f. C'est la définition de la surjectivité.

Donc chaque élément possède un antécédent donc f est surjective.

injective ?

On suppose que $f(n) = f(m)$, pour n,m. On distingue 2 cas.

1) [n et m sont de parités différentes] Si n est pair et m est impair,
   $f(n) = f(m) \Leftrightarrow n + 1 = m - 1 \Leftrightarrow m = n + 2$
   $\to$ m est pair $\to$ contradiction
   D'après ce raisonnement par l'absurde, on déduit qu'on ne considère pas le cas où n et m sont de parités différentes pour déterminer si f est injective.
2) Si n et m sont de même parité :
   on obtient $\left.\begin{matrix} (\text{pairs}) & n+1 = m+1 \\ (\text{impairs}) & n-1 = m-1 \end{matrix}\right\} n = m$

Donc f est injective et bijective.

(e) $f : A^* \to A^*$ telle que $f(u) = u.b$ où $A = \{a, b\}$

A^* : langage défini sur A (ensemble des mots composés de a et b + mot vide ε)

u : mot

b : suffixe

$\begin{cases} u = abba \\ f(u) = abbab \end{cases}$

injective ? oui

si $f(u) = f(v)$, $u.\cancel{b} = v.\cancel{b} \to u = v$

Si on enlève le « $.b$ » (suffixe qui ne change pas), on obtient : $u = v$.

surjective ? non

$\to$ le mot vide ε n'a pas d'antécédent

$\to$ les mots finissant par $\boldsymbol{a}$ n'ont pas d'antécédent

3. Combien existe-t-il d'applications de $\{a, b, c\}$ dans $\{1,2\}$? Combien sont des applications injectives ? des applications surjectives ? des applications bijectives ?

applications de $\{a, b, c\}$ dans $\{1,2\}$

- 1 ou 2 n'a pas d'antécédent. → non surjectives
  - $f_1(a) = f_1(b) = f_1(c) = 1$
  - $f_2(a) = f_2(b) = f_2(c) = 2$
- 1 a un antécédent et 2 a deux antécédents.
  - $f_3(a) = 1, f_3(b) = f_3(c) = 2$
  - $f_4(b) = 1, f_4(a) = f_4(c) = 2$
  - $f_5(c) = 1, f_5(a) = f_5(b) = 2$
- 1 a deux antécédents et 2 a un antécédent.
  - $f_6(b) = f_6(c) = 1, f_6(a) = 2$
  - $f_7(a) = f_7(c) = 1, f_7(b) = 2$
  - $f_8(a) = f_8(b) = 1, f_8(c) = 2$

8 applications : 2^3 de $\{a, b, c\}$ dans $\{1,2\}$

A chaque fois, il existe plusieurs antécédents pour une même image donc aucune application n'est injective, ni bijective.

6 applications sont surjectives.

Exercice 12. Applications entre ensembles finis

Soient E et F deux ensembles finis non vides contenant respectivement p et n éléments.

1. Montrer que le nombre d'applications de E vers F est n^p.

Par récurrence sur p

→ Cas de base : $p = 1$. On a alors 1 seul élément dans E, $E = \{e\}$, et pour choisir l'image de e dans F, on a $n = n^1$ différents choix. ⇒ n^p applications avec $p = 1$

→ Etape de récurrence

On suppose que le nombre d'applications de E vers F est n^p avec $|E| = p$ et $|F| = n$.

On montre que si on ajoute un élément dans E, le nombre d'applications de E vers F est n^{p+1} (avec $|E| = p + 1$ et $|F| = n$).

Si E contient $p + 1$ éléments, on peut l'écrire sous la forme $E = \{e\} \cup E'$, et donc $|E'| = p$ car $e \notin E'$.

Alors par hypothèse de récurrence, on a n^p applications de E' vers F.

Pour chacune de ces applications, on a n possibilités de choisir l'image de e dans F.

Donc pour $E = \{e\} \cup E'$ de cardinalité $p + 1$, le nombre d'applications est $\underbrace{n \cdot n^p}_{*} = n^{p+1}$ de E vers F.

* pour e dans chacune des n^p applications

2. Combien d'applications de $\{0,1\}$ vers $\{0,1\}$ peut-on construire ? Montrer que pour toute application $\{0,1\}$ vers $\{0,1\}$, $f\left(f\left(f(x)\right)\right) = f(x)$.

D'après la question précédente, le nombre d'applications de $\{0,1\}$ vers $\{0,1\}$ est $2^2 = 4$ applications.

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	0	1
1	1	1	0	1

On vérifie que $f_1\left(f_1\left(f_1(x)\right)\right) = f_1(x)$:

Si $x = 0$, $f_1(0) = 0 \Rightarrow f_1\left(f_1(0)\right) = f_1(0) = 0 \Rightarrow f_1\left(f_1\left(f_1(0)\right)\right) = f_1(0)$

Si $x = 1$, $f_1(1) = 1 \Rightarrow f_1\left(f_1(1)\right) = f_1(1) = 1 \Rightarrow f_1\left(f_1\left(f_1(1)\right)\right) = f_1(1)$

Donc $f_1\left(f_1\left(f_1(x)\right)\right) = f_1(x)$.

??? vérifier manuellement que $f_2\left(f_2\left(f_2(x)\right)\right) = f_2(x)$, pareil pour f_3 et f_4

Exercice 15. Involutions

On dit qu'une application $f : E \to E$ est une involution si et seulement si pour tout $x \in E$, $f\left(f(x)\right) = x$. Montrer que si f est une involution alors f est bijective.

On suppose que f est une involution, c'est-à-dire que $\forall x \in E$, $f\left(f(x)\right) = x$.

Injective ? Si $x_1, x_2 \in E$ sont tels que $f(x_1) = f(x_2)$, alors on sait que $f\left(f(x_1)\right) = f\left(f(x_2)\right)$ et puisque f est involutive, $x_1 = x_2$, et donc f est <u>injective</u>.

Surjective ? Soit $x \in E$. Comme f est involutive, $x = f\left(f(x)\right)$, et donc x admet bien un antécédent $f(x) \in E$ par f et donc f est <u>surjective</u>.

f est injective et surjective donc f est bijective.

Exercice 16. Composition d'applications

Soit $f : A \to B$ et $g : B \to C$ deux applications.

1. Montrer que si $g \circ f$ est injective alors f est injective.

$\underbrace{A}_{x} \xrightarrow{f} \underbrace{B}_{y} \xrightarrow{g} \underbrace{C}_{z}$ $\qquad g \circ f = g\left(f(x)\right)$

On suppose que $g \circ f$ est injective.

Soit $x_1, x_2 \in A$ tel que $f(x_1) = f(x_2)$.

Il vient que $g\left(f(x_1)\right) = g\left(f(x_2)\right)$ et donc $x_1 = x_2$ (car, par hypothèse, $g \circ f$ est injective).

Donc f est injective.

2. Montrer que si $g \circ f$ est surjective alors g est surjective.

Soit $z \in C$ (une image finale dans C).

Puisque $g \circ f$ est surjective (par hypothèse), il existe un élément $x \in A$ tel que $g\left(f(x)\right) = z$ (x est l'*ante*-antécédent de z.)

et donc il existe un élément $y = f(x) \in B$, tel que $z = g(y)$,
d'où on conclut que g est <u>surjective</u>.

Exercice 17. Bijection réciproque

On rappelle que pour une application $f : E \to F$, une partie A de E et une partie B de F, on définit $f(A) = \{y \in F | \exists x \in A, y = f(x)\}$ et $f^{-1}(B) = \{x \in E | f(x) \in B\}$.

1. Montrer que pour toute partie A de E, $A \subseteq f^{-1}(f(A))$.

pour toute partie A de E : $A \subseteq E$

Soit $x \in A$, alors $f(x) \in f(A)$ et donc $x \in f^{-1}(f(A))$.

TD 2 : Ensembles ordonnés, relations d'ordre

Rappels de cours

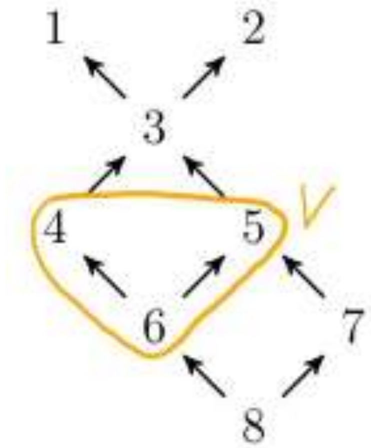
$(E, \preccurlyeq)$ ensemble

X partie de E

- **Éléments minimaux de X :** $x \in X$ tel que $\nexists$ dans X des éléments plus petit que X
- **Éléments maximaux de X :** $x \in X$ tel que $\nexists$ dans X des éléments plus grand que X
- **Minorants de X :** $e \in E$ tel que $e \preccurlyeq$ tous les éléments de X
- **Majorants de X :** $e \in E$ tel que $e \succcurlyeq$ tous les éléments de X
- **Plus petit élément :** $X \cap$ majorants(X)
- **Plus grand élément :** $X \cap$ minorants(X)

Exercice 1. Majorants, minorants, borne supérieure, borne inférieure

Soit $W = \{1, 2, 3, 4, 5, 6, 7, 8\}$ un ensemble ordonné selon le diagramme suivant :



On considère le sous-ensemble $V = \{4, 5, 6\}$ de W.

1. Trouver l'ensemble des majorants de V.

Majorants de $V = \{1, 2, 3\}$

2. Trouver l'ensemble des minorants de V.

Les minorants sont des éléments de E, n'appartenant pas forcément à V, qui sont plus petit que tous les éléments de V.

Minorants de $V = \{6, 8\}$

7 ne l'est pas car 4 et 7 / 6 et 7 incomparables. Il n'y a pas d'arc entre 4 et 7, et 6 et 7.

6 est plus petit que 4 et 5, et plus petit ou égal à lui-même. 8 est plus petit que 6, donc par transitivité plus petit que 4 et 5 (on ne dessine pas les grands arcs de transitivité sur le graphe couvrant d'une relation).

3. Est-ce que $\sup(V)$ existe ?

$\underbrace{\sup(V) = 3}_{3 \notin V}$ car 3 est le plus petit des majorants

4. Est-ce que $\inf(V)$ existe ?

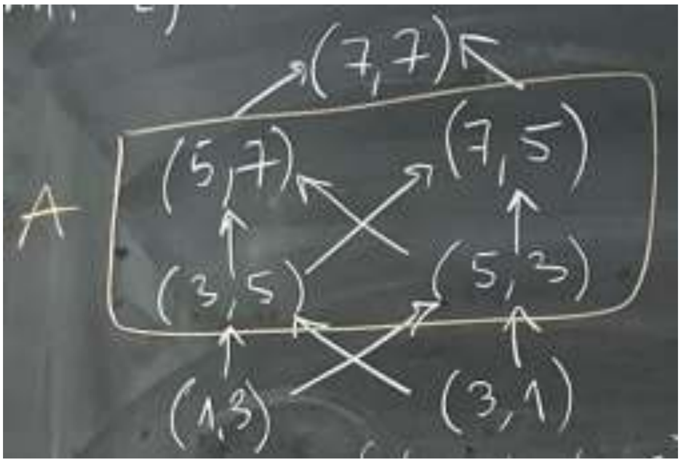
$\underbrace{\inf(V) = 6}_{6 \in V}$ car 6 est le plus grand des minorants

Exercice 2

Soit R la relation définie sur l'ensemble $E = \{(1,3), (3,1), (3,5), (5,3), (5,7), (7,5), (7,7)\}$ par : $(m_1, m_2) R (n_1, n_2)$ si et seulement si $m_1 \leq n_1$ et $m_2 \leq n_2$

Pour l'ensemble $A = \{(3,5), (5,3), (5,7), (7,5)\}$ donner, s'ils existent les éléments maximaux, les éléments minimaux, les majorants, les minorants, le plus grand élément, le plus petit élément, la borne inférieure et la borne supérieure.

On construit le graphe couvrant de R à partir de l'expression mathématique de la relation :



Eléments minimaux : $\{(3,5), (5,3)\}$

Eléments maximaux : $\{(5,7), (7,5)\}$

Minorants : $\{(1,3), (3,1)\}$

Majorants : $\{(7,7)\}$

Plus petit élément : $\emptyset$

Plus grand élément : $\emptyset$

$\inf(A)$: $\emptyset$ (car $\inf(A)$ est un unique élément, et $(1,3)$ et $(3,1)$ sont incomparables)

$(1,3)$ et $(3,1)$ sont tous les deux des minorants de A, mais on ne peut pas déterminer le quel est le plus grand car ils sont incomparables (ils ne sont pas en relation).

$\sup(A)$: $(7,7)$

Exercice 3

On définit la relation $\preccurlyeq \subseteq \mathbb{N} \times \mathbb{N}$ par $(a, b) \preccurlyeq (c, d)$ ssi $a + b < c + d$ ou $(a, b) = (c, d)$.

1. Montrer que $\preccurlyeq$ est une relation d'ordre.

<u>Réflexive :</u> soit $(a, b) \in \mathbb{N}^2$

Comme $(a, b) = (a, b)$ ($a = a$ et $b = b$), $\preccurlyeq$ est réflexive.

<u>Anti-symétrique :</u> soient $(a, b), (c, d) \in \mathbb{N}^2$ tels que $(a, b) \preccurlyeq (c, d)$ et $(c, d) \preccurlyeq (a, b)$

Alors puisque $a + b < c + d$ et $c + d < a + b$ ne peuvent pas être vrais, simultanément, on a forcément $(a, b) = (c, d)$.

<u>Transitive :</u> soient $(a,b),(c,d),(e,f) \in \mathbb{N}^2$ et $(a,b) \preccurlyeq (c,d)$ et $(c,d) \preccurlyeq (e,f)$

2 cas possibles

1. si $a+b<c+d$:
   1.1. si $c+d<e+f$: alors $a+b<e+f$, donc $(a,b) \preccurlyeq (e,f)$
   1.2. si $(c,d)=(e,f)$, comme $(a,b) \preccurlyeq \underbrace{(c,d)}_{=(e,f)}$ on a $(a,b) \preccurlyeq (e,f)$
2. si $(a,b)=(c,d)$: comme $\underbrace{(c,d)}_{=(a,b)} \preccurlyeq (e,f)$, on a $(a,b) \preccurlyeq (e,f)$

Lorsqu'on n'autorise pas l'égalité (relation stricte), la relation n'est pas une relation d'ordre car elle n'est pas réflexive (un élément ne peut pas être en relation avec lui-même).

2. Cet ordre est-il total ? bien fondé ? Justifier les réponses.

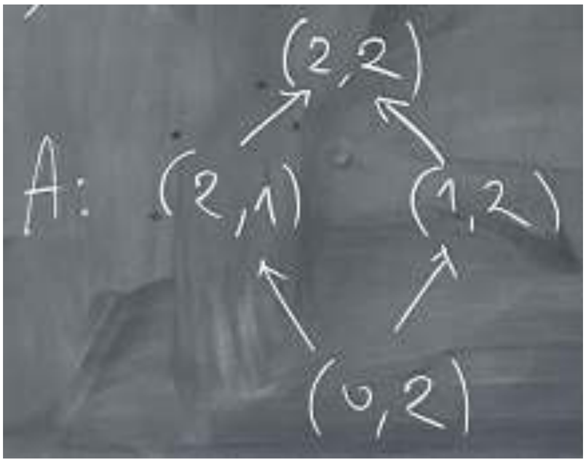
Ordre total ? <u>non</u>

Si $a+b=c+d$ et $a=d$ et $b=c$, par exemple $(2,3)$ et $(3,2)$ ne sont pas comparables

Bien fondé ? <u>oui</u>

$(0,0)$ est l'élément minimal

3. Soit l'ensemble $A=\{(0,2),(2,1),(1,2),(2,2)\}$. Déterminer, s'ils existent, les minorants, les majorants, les éléments minimaux, les éléments maximaux, la borne inférieure, la borne supérieure, le minimum, le maximum de A.



Eléments minimaux : $\{(0,2)\}$

Eléments maximaux : $\{(2,2)\}$

Minorants : $\{\{(0,2)\} \cup \{(x,y) \text{ tel que } x+y<2\}\}$

$\uparrow$ en dehors de A $\downarrow$

Majorants : $\left\{\{(2,2)\} \cup \underbrace{\{(x,y) \text{ tel que } x+y>4\}}_{\{(0,0),(0,1),(1,0)\}}\right\}$

Plus petit élément : $(0,2)$

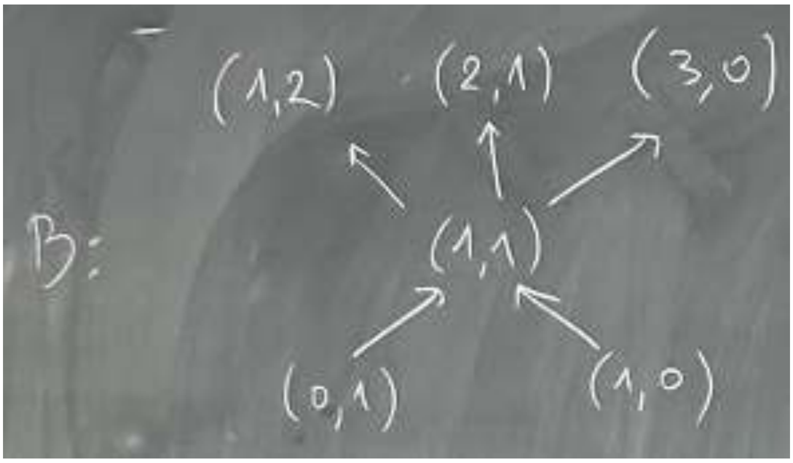
Plus grand élément : $(2,2)$

$\inf(A)$: $(0,2)$

$\sup(A)$: $(2,2)$

4. Même question pour $B = \{(0,1), (1,0), (1,1), (1,2), (2,1), (3,0)\}$

$(0,1)$ et $(1,0)$ ne sont pas comparables. Leur somme fait 1, elle est inférieure à la somme des autres couples donc ils sont en bas du graphe.



Eléments minimaux : $\{(0,1), (1,0)\}$

Eléments maximaux : $\{(1,2), (2,1), (3,0)\}$

Minorants : $\{(0,0)\}$

Majorants : $\{(x, y) \text{ tel que } x + y > 3\}$

Plus petit élément : aucun

Plus grand élément : aucun

$\inf(A)$: $(0,0)$

$\sup(A)$: aucun

Exercice 4

Soit $E = \{2, 3, 4, \cdots\} = \mathbb{N} \setminus \{0,1\}$, ordonné par la relation « x divise y ».

1. Vérifier que cette relation est une relation d'ordre.

<u>Réflexive :</u> $\forall x \in E$, x divise x

<u>Anti-symétrique :</u> soient $x, y \in E$

si x divise y et y divise x, alors on peut écrire

$y = k \cdot x$ avec $k \in \mathbb{N} \setminus \{0\}$ et $x = m \cdot y$ avec $m \in \mathbb{N} \setminus \{0\}$

On substitue x par sa valeur dans $y = k \cdot x$.

$\Rightarrow y = k \cdot m \cdot y \Leftrightarrow y(1 - km) = 0$ et on sait que $y \neq 0$

donc $1 - km = 0 \Leftrightarrow km = 1$

donc $k = m = 1$

On obtient $x = y$.

<u>Transitive :</u> si $\underbrace{x \text{ divise } y}_{y=k\cdot x}$ et $\underbrace{y \text{ divise } z}_{z=m\cdot y}$, $z = m \cdot \underbrace{k \cdot x}_{=y}$ donc x divise z

2. Déterminer les éléments minimaux de E.

pour les <u>nombres premiers</u> ($p \in E$), seulement p divise p

$\Rightarrow$ tous les nombres premiers sont des élément minimaux (noter que $1 \notin E$)

3. Déterminer les éléments maximaux de E.

Il n'y en a pas, car pour chaque $x \in E$, x divise $2x$, ou $3x$, etc. (on peut toujours construire des éléments supérieurs dans le sens de la relation « divise »).

Exercice 5

On se place dans $F = \mathbb{N} \setminus \{0\}$ ordonné par la relation « x divise y ».

1. Existe-t-il une borne supérieure et une borne inférieure pour tout sous-ensemble de 2 éléments ?

inf et sup pour tout $\{x, y\}$

Pour tout $\{x, y\}$ tel que $x, y \in F$,

majorants de $\{x, y\}$ = tous les nombres divisibles par x et y

minorants de $\{x, y\}$ = tous les nombres qui divisent x et y

inf : pgcd(x, y) (plus grand des minorants)

sup : ppcm(x, y) (plus petit des majorants)

ppcm → plus petit commun multiple

2. Soient les ensembles $A = \{6, 15, 21\}$ et $B = \{1, 6, 14, 21\}$. Donner les minorants et les majorants de A (resp. B). A (resp. B) possède-t-il un plus petit élément ? un plus grand élément ?

	$A = \{6, 15, 21\}$	$B = \{1, 6, 14, 21\}$
minorants	ppcm (210) et ses multiples	42 et ses multiples
majorants	pgcd (3) et ses diviseurs (1 et 3)	1
plus petit élément	aucun	1
plus grand élément	aucun	aucun ($42 \notin B$)

Calcul de ppcm$(6, 15, 21)$:

$$\begin{array}{ccc|c} 6 & 15 & 21 & 3 \\ 2 & 5 & 7 & \end{array}$$

2, 5 et 7 sont premiers entre eux.

On divise 6, 15 et 21 par des diviseurs communs aux trois nombres jusqu'à atteindre un triplet de nombres premiers entre eux. Le ppcm est le produit du triplet.

Calcul de ppcm$(1, 6, 14, 21)$:

$$\begin{array}{cccc|c} (1) & 6 & 14 & 21 & 2 \\ & 3 & 7 & 21 & 3 \\ & (1) & 7 & 7 & 7 \\ & & (1) & (1) & \end{array}$$

On divise par des diviseurs communs (pas forcément à tous les nombres) jusqu'à obtenir uniquement des 1. Le produit des nombres dans la colonne de droite est le ppcm.

3. Soit $A = \{3, 6, 12, 15\}$. Donner les majorants, minorants, la borne supérieure, la borne inférieure, le plus petit et le plus grand élément, les éléments maximaux, minimaux s'ils existent. Discuter.

	$C = \{3, 6, 12, 15\}$
minorants	$\text{ppcm} = 2 \cdot 2 \cdot 3 \cdot 5 = 60$ et ses multiples
majorants	$\text{pgcd} = 3$ et 1
plus petit élément	3
plus grand élément	aucun ($60 \notin C$)

Calcul de ppcm$(3, 6, 12, 15)$:

$$\begin{array}{cccc|c} 3 & 6 & 12 & 15 & 3 \\ (1) & 2 & 4 & 5 & 2 \\ & (1) & 2 & 5 & 2 \\ & & (1) & 5 & 5 \\ & & & (1) & \end{array}$$

$\sup = 60$

$\inf = 3$

élément maximum = $\{12, 15\}$ (aucun élément <u>dans C</u> n'est un multiple de 12 et de 15 sans leur être égal)

élément minimum = $\{3\}$ (aucun élément <u>dans C</u> n'est diviseur de 3 sans lui être égal)

Exercice 6

Donner un exemple d'ensemble ordonné qui a exactement un élément maximal mais qui n'a pas de plus grand élément.

$E = \{2^n, n \geq 1\} \cup \{3\}$, « divise »

Graphe couvrant :

$$\begin{array}{cc} \vdots & \\ 2^3 & \\ \uparrow & \\ 2^2 & \\ \uparrow & \\ 2 & \mathbf{3} \end{array}$$

Remarque : 2 et 3 sont les éléments minimaux.

3 est le seul élément maximal (car il n'existe pas <u>dans</u> <u>E</u> d'éléments strictement supérieurs à 3)

$\downarrow$

car 3 n'est même pas comparable avec le reste (autres éléments de E)

mais on n'a pas de plus grand élément (car on peut toujours construire une puissance de 2 supérieure multiple des puissances précédentes)

Autre exemple artificiellement construit :

$F = \{a, 1, 2, 3, \cdots\} = \{a\} \cup \mathbb{N} \setminus \{0\}$

relation $\preccurlyeq$ dans le sens d'entiers naturels

a est l'unique élément maximal mais il n'existe pas d'élément plus grand élément (raisonnement identique).

$$\begin{array}{cc} \vdots & \\ 3 & \\ \uparrow & \\ 2 & \\ \uparrow & \\ 1 & \boldsymbol{a} \end{array}$$

Exercice 8

Langages

A est un alphabet (exemples : $A = \{a\}, A = \{a, b, \cdots\}$).

A^* est un langage défini sur A avec des mots de n'importe quelle longueur.

<u>Exemple :</u> $A = \{a, b\}$

$A^* = \{\varepsilon, a, b, aa, ab, ba, bb, aaa, bbb, \cdots\}$

$\varepsilon \to$ notation du mot vide

Notations usuelles :

- u, v, w pour des lettres ou des mots
- $\preccurlyeq_{\text{pref}}$ pour la relation « est un préfixe de »

1. Définir la relation « est un préfixe de » sur A^*. S'agit-il d'une relation d'ordre ? si oui, s'agit-il d'un ordre total ou d'un ordre partiel ?

Relation « est un préfixe de » ($\preccurlyeq_{\text{pref}}$) $\to$ <u>ordre partiel</u>

- informel : le mot x est un préfixe du mot y si et seulement si x est le « début » de y
- formel : $u_1 u_2 \cdots u_n \preccurlyeq_{\text{pref}} v_1 v_2 \cdots v_m \Leftrightarrow n \leq m$ et $\forall i \leq n, u_i = v_i$

Exemple : $\underbrace{\text{bon}}_{3} \preccurlyeq_{\text{pref}} \underbrace{\text{bonjour}}_{7}$ $\underbrace{\text{bon}}_{3} \preccurlyeq_{\text{pref}} \underbrace{\text{bonsoir}}_{7}$ On a bien $3 < 7$.

2. En supposant que A est muni d'un ordre total $\preccurlyeq_A$, définir l'ordre lexicographique sur A^*. S'agit-il d'un ordre total ou d'un ordre partiel ?

A muni de $\preccurlyeq_A$ (exemple : ordre alphabétique : $a \preccurlyeq_A b \preccurlyeq_A c \cdots \preccurlyeq_A z$)

Définir $\preccurlyeq_{\text{lex}}$ sur A^*

Soient $u = u_1 u_2 \cdots u_n$ et $v = v_1 v_2 \cdots v_m$ 2 mots de A^*.

On dit $u \preccurlyeq_{\text{lex}} v$ si et seulement si

- soit u est un préfixe de v : $u \preccurlyeq_{\text{pref}} v$
- soit u et v sont coïncidents (les mêmes) jusqu'à une position i ($u_1 u_2 \cdots u_i = v_1 v_2 \cdots v_i$) et que à la position suivante $\underbrace{u_{i+1} \neq v_{i+1}}_{\text{les lettres diffèrent}}$ et $\underbrace{u_{i+1} \preccurlyeq_A v_{i+1}}_{\downarrow}$

la lettre u_{i+1} se trouve avant v_{i+1} dans l'alphabet A

$u \preccurlyeq_{\text{lex}} v \to$ <u>ordre total</u> (car on peut comparer tous les mots à n'importe quel moment)

3. Soit $A = \{a, b\}$ tel que $a \preccurlyeq_{\text{lex}} b$. Montrer que l'ordre lexicographique défini à la question précédente n'est pas un ordre bien fondé.

suite infinie strictement décroissante

$(a^n b)$ avec $n \in \mathbb{N}$

Il n'existe pas d'élément minimal car on peut toujours construire un élément plus petit en rajoutant un a au début du mot.

ab
aab
$aaab$
$aaaab$
$\vdots$
$\vdots$
$\downarrow$

Exercice 9

Les ordres suivant sont-ils bien fondés ?

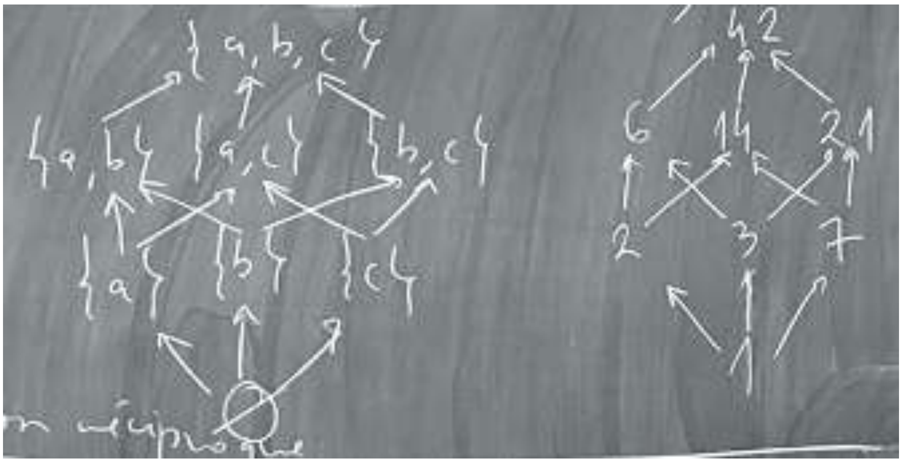
Tous sont bien fondés sauf le 6. ??? à réfléchir pour la semaine prochaine

Exercice 10

Montrer que les ensembles ordonnés $\mathcal{P}(\{a, b, c\})$ muni de la relation d'inclusion et $\{1, 2, 3, 6, 7, 14, 21, 42\}$ muni de la relation de division (dans $\mathbb{N}$) sont isomorphes.

$(\mathcal{P}(\{a, b, c\}), \subseteq)$ et ($\{1, 2, 3, 6, 7, 14, 21, 42\}$, division) isomorphes ?

$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$



Les graphes couvrants sont de même forme donc les ensembles sont isomorphes.

Méthode : Pour prouver que les deux ensembles sont isomorphes, il faut définir la bijection et prouver que f et f^{-1} sont monotones.

On écrit maintenant la bijection :

$f : E \to F$

$$\begin{array}{l|l} f(\emptyset) = 1 & f(\{a, b\}) = 6 \\ f(\{a\}) = 2 & f(\{a, c\}) = 14 \\ f(\{b\}) = 3 & f(\{b, c\}) = 21 \\ f(\{c\}) = 7 & f(\{a, b, c\}) = 42 \end{array}$$

$\to f(A \cup B) = f(A) \cdot f(B), \quad A, B \subseteq E$

$f^{-1} : F \to E$

$f^{-1}(1) = \emptyset \qquad f^{-1}(2) = \{a\} \qquad f^{-1}(3) = \{b\} \qquad f^{-1}(7) = \{c\}$

$f^{-1}(x \cdot y) = f^{-1}(x) \cup f^{-1}(y), \quad x, y \in F$

On prouve la monotonie :

Monotonie de f : si $A \subseteq B$, alors $A \cup B = B$

donc $f(B) = \underbrace{f(A \cup B)}_{f(A) \cdot f(B)}$ et $f(A)$ divise $f(B)$

Monotonie de f^{-1} : si x divise y, alors $y = kx$,

donc $f^{-1}(y) = f^{-1}(x) \cup f^{-1}(k)$

et donc $f^{-1}(x) \subseteq f^{-1}(y)$

Exercice 11

Soit E un ensemble muni d'une relation d'ordre $\preccurlyeq$ et soit A une partie de E.

1. Montrer que si A admet un plus grand élément alors cet élément est l'unique élément maximal. La réciproque est-elle vraie ? Justifier.

Existence : On suppose que A admet un plus grand élément $M \in A$.

Par définition des majorants, pour tout $a \in A$, $a \preccurlyeq M$.

Donc par antisymétrie de $\preccurlyeq$, $\forall a \in A$, si $M \preccurlyeq a$, alors $M = a$ et M est l'élément maximal (définition de l'élément maximal).

On prouve qu'il n'existe pas un élément plus grand que M par antisymétrie. A chaque fois qu'on essaie de trouver a plus grand que M, on voit qu'il est égal à M par antisymétrie.

Unicité : On suppose qu'il existe un autre élément maximal M'.

Alors, comme $\underbrace{M' \preccurlyeq M}_{\text{car } M \text{ est le plus grand élément}}$, mais comme M' est un élément maximal, alors $M = M'$.

Il ne peut pas y avoir plusieurs éléments maximaux donc $M = M'$.

La réciproque serait : si A admet un unique élément maximal, alors A admet un plus grand élément.

La réciproque n'est pas vraie (voir Exercice 6 pour contre-exemple).

2. On suppose que la relation d'ordre $\preccurlyeq$ est *totale*. Montrer qu'alors, si A admet un élément maximal, cet élément est unique. Montrer de plus que dans ce cas, cet élément maximal est le plus grand élément de A.

Supposons que A admet un élément maximal M.

Alors, pour tout $a \in A$, si $M \preccurlyeq a$, alors $M = a$ (par antisymétrie de $\preccurlyeq$).

Supposons qu'il existe un autre élément maximal M'.

Si $M \preccurlyeq M'$, alors $M = M'$. (par définition de l'élément maximal)

Sinon, comme l'ordre est total, on a $M' \preccurlyeq M$ et $M' = M$.

Dans les deux cas, on arrive à la conclusion que M est l'unique élément maximal de A.

Montrer que M est aussi un majorant de A :

Soit $a \in A$, si $M \preccurlyeq a$ alors $M = a$. (par def des majorants)

Comme l'ordre est total, on déduit que $\forall a \in A$, $a \preccurlyeq M$.

On déduit que tout élément de A est soit égal soit plus petit que M.
Donc M est un majorant de A dans A, donc M est le plus grand élément.

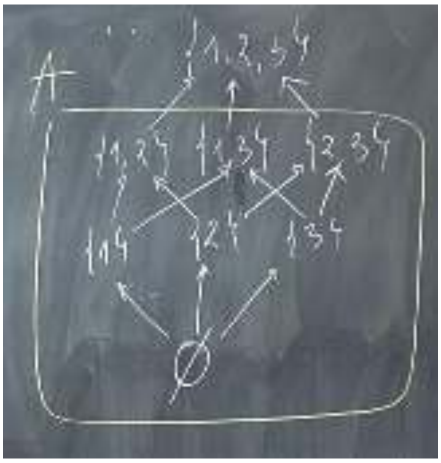
Exercice 16

1. On note $\mathcal{P}(\mathbb{N})$ l'ensemble des sous-ensembles de $\mathbb{N}$. On considère les deux ensembles ordonnés $(\mathcal{P}(\mathbb{N}), \subseteq)$ et $(\mathbb{N}, \leq)$, où $\subseteq$ est la relation d'inclusion d'ensembles, et $\leq$ et la relation d'ordre usuelle sur les entiers naturels. On définit une application $f : \mathcal{P}(\mathbb{N}) \to \mathbb{N}$ par $f(X) = \sum_{x\in X} x$, pour tout $X \in \mathcal{P}(\mathbb{N})$. L'application f est-elle monotone.

Soient $\underbrace{A, B \subseteq N}_{A,B\in\mathcal{P}(\mathbb{N})}$ tels que $A \subseteq B$. A est plus petit que B dans le sens de l'inclusion.

Alors $f(A) = \sum_{a\in A} a \leq \sum_{a\in A} a + \sum_{b\in B\setminus A} b = \sum_{b\in B} b = f(B)$ $f(A) \leq f(B)$ dans le sens usuel.
donc f est monotone.

2. Soit le sous-ensemble $E = \mathcal{P}(\{1, 2, 3\})$ de $\mathcal{P}(\mathbb{N})$, ordonné par la relation d'inclusion d'ensembles.
   (a) Représenter la relation d'ordre par un graphe (sans les arcs de réflexivité ni de transitivité).



   (b) Pour la partie $A = E \setminus \{1, 2, 3\}$, donner l'ensemble des majorants et l'ensemble des minorants. Donner, lorsqu'ils existent, la borne inférieure, la borne supérieure, le plus petit élément et le plus grand élément. S'ils n'existent pas, indiquer « n'existe pas ». Donner les éléments minimaux et les éléments maximaux.

majorants $(A) = \{\{1, 2, 3\}\}$
minorants $(A) = \{\emptyset\}$
$\sup(A) = \{1, 2, 3\}$
$\inf(A) = \emptyset$
plus grand élément : n'existe pas
plus petit élément $= \emptyset$
éléments maximaux : $\{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$
éléments minimaux : $\{\emptyset\}$

3. Soient $(E, \preccurlyeq_1)$ et $(F, \preccurlyeq_2)$ deux ensembles ordonnés, et soit $f : E \to F$ une application monotone. Soit A une partie de E. On note $f(A) = \{f(x) \mid x \in A\}$.
   (a) Montrer que si A admet un plus grand élément M, alors $f(M)$ est le plus grand élément de $f(A)$.

$f : E \to F$ monotone signifie $x \preccurlyeq_1 y \ (x, y \in E) \Rightarrow f(x) \preccurlyeq_2 f(y)$

Par définition du plus grand élément, $M \in A$. Donc $f(M) \in f(A)$.

Soit $y \in f(A)$, alors $\exists x \in A$ tel que $f(x) = y$, et $x \preccurlyeq_1 M$.

Comme f est monotone, $f(x) \preccurlyeq_2 f(M)$.

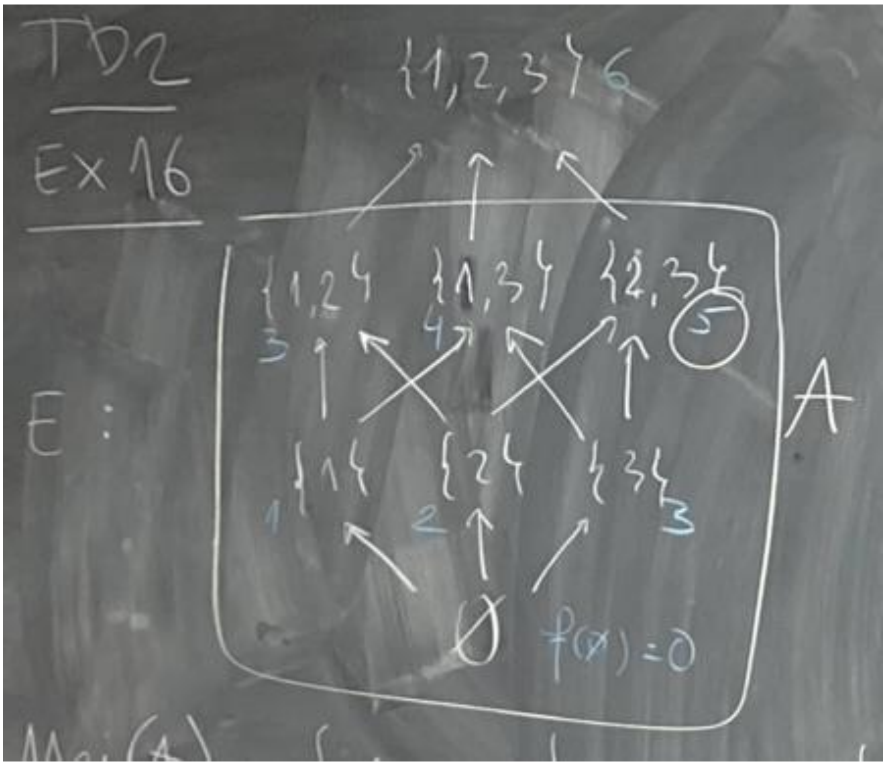
On a prouvé que pour un x quelconque, $f(x) \preccurlyeq_2 f(M)$, ce qui est la définition du plus grand élément.

Donc $f(M)$ est le plus grand élément de $f(A)$.

   (b) Peut-on affirmer que si A admet une borne supérieure B, alors $f(B)$ est la borne supérieure de $f(A)$? On pourra s'inspirer de l'application f définie à la question 1, et de la partie A définie à la question 2.

Question 1 : $f(X) = \sum_{x \in X} x$

Question 2 : On applique f (image = somme des éléments de l'ensemble) à la partie A :



La borne supérieure de A est $\{1, 2, 3\}$.

Dans $f(A)$: $f(\{2, 3\}) = 5$ est bien un majorant de $f(A)$, et il est le plus petit majorant car $5 < 6$.

Donc la **borne supérieure** (par définition, le plus petit majorant) de $f(A)$ est 5, et la propriété est fausse.

TD 3 : Induction sur $\mathbb{N}$

Rappel : Induction

Induction (simple)	**Induction forte (ou généralisée)**
Soit $P(n)$ une propriété. Si $\begin{cases} P(0) \text{ est vraie} \\ \forall n \geq 0, P(n) \Rightarrow P(n+1) \end{cases}$ alors $\forall n \in \mathbb{N}$, P(n) est vraie. cas de base étape d'induction	Soit $P(n)$ une propriété. Si $\begin{cases} P(0) \text{ est vraie} \\ \forall n \geq 0, \forall k \leq n, P(k) \text{ vraie, alors } P(n) \text{ vraie} \end{cases}$ alors $\forall n \in \mathbb{N}$, P(n) est vraie. cas de base induction générale

Exercice 1

Montrer que, pour $n \geq 2$,

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}$$
$$\overline{A_1 \cap A_2 \cap \cdots \cap A_n} = \overline{A_1} \cup \overline{A_2} \cup \cdots \cup \overline{A_n}$$

(Lois de De Morgan généralisées)

Lois de De Morgan : $\overline{A \cup B} = \bar{A} \cap B$ $\quad \overline{A \cap B} = \bar{A} \cup \bar{B}$

Par induction :

<u>Cas de base :</u> $n = 2$, $\left.\begin{array}{l} \overline{A_1 \cup A_2} = \overline{A_1} \cap \overline{A_2} \\ \overline{A_1 \cap A_2} = \overline{A_1} \cup \overline{A_2} \end{array}\right\}$ De Morgan

donc $P(2)$ est vraie.

<u>Induction :</u> $P(n) \Rightarrow P(n+1)$

On suppose que $P(n)$ est vraie (hypothèse d'induction).

1) $\overline{A_1 \cup \cdots \cup A_n} = \overline{A_1} \cap \cdots \overline{A_n}$

Soit $A = \overline{A_1 \cup \cdots \cup A_n}$.

Au rang $n+1$, $P(n+1)$: $\overline{A \cup A_{n+1}} = \bar{A} \cap \overline{A_{n+1}}$ (loi de De Morgan)

Par hypothèse d'induction, $\bar{A} = \overline{A_1} \cap \cdots \overline{A_n}$.

En remplaçant $\bar{A}$, $P(n+1)$ devient $\overline{\underbrace{A \cup \cdots \cup A_n}_{A} \cup A_{n+1}} = \underbrace{\overline{A_1} \cap \cdots \overline{A_n}}_{\bar{A}} \cap \overline{A_{n+1}}$

<u>Conclusion :</u> $\forall n \geq 2$, $P(n)$ est vraie.

2) $\overline{A_1 \cap \cdots \cap A_n} = \overline{A_1} \cup \cdots \cup \overline{A_n}$: même raisonnement (on inverse $\cap$ et $\cup$)

Exercice 2

Soit a un entier. Soit $P_a(n)$ la propriété « $9 \mid (10^n + a)$ ». Montrer que, pour tout entier a et tout $n \in \mathbb{N}$, $P_a(n)$ implique $P_a(n+1)$. A-t-on $P_a(n)$ pour tout $n \in \mathbb{N}$?

$\forall a \in \mathbb{Z}$, $P_a(n)$: « 9 divise $10^n + a$ »

Montrer que $\forall n \in \mathbb{N}$, $P(n) \Rightarrow P(n+1)$

hypothèse d'induction $\qquad$ 9 divise $10^{n+1} + a = 10^n \cdot 10^1 + a$

On suppose que 9 divise $10^n + a$. On peut l'écrire $9k$.

Est-ce qu'on peut écrire $10^n \cdot 10^1 + a$ comme $9 \cdot l$.

La différence entre $P_a(n+1)$ et $P_a(n)$: $(10^{n+1} + a) - (10^n + a)$

$= (10^n \cdot 10 + \cancel{a}) - (10^n + \cancel{a}) = 10 \cdot 10^n - 1 \cdot 10^n = \mathbf{9} \cdot 10^n$

Donc $P_a(n)$ implique $P_a(n+1)$.

Pour que P soit vraie $\forall n \in \mathbb{N}$ et $\forall a \in \mathbb{Z}$, il faut qu'elle soit vraie en $n = 0$.

$P(0)$: « 9 divise $\underbrace{10^0}_{1} + a$ »

donc 9 divise $a + 1$

$a + 1 \equiv 0 \text{ mod } 9 \Rightarrow a \equiv -1 \text{ mod } 9$

donc $a = \underbrace{8}_{-1} \text{ mod } 9$

C'est le cas pour $a = 8$ ou $a = -1$, mais pas pour $a = 1$, ou 2, etc.

Donc le cas de base n'est pas vrai $\forall a \in \mathbb{Z}$.

Le cas de base est vrai pour les entiers appartenant à la même classe d'équivalence que 8 mod 9.

Exercice 3

La suite harmonique est définie par $H_n = 1 + \frac{1}{2} + \cdots + \frac{1}{n}$ pour $n \geq 1$.

1. Montrer que $H_{2^n} \geq 1 + \frac{n}{2}$.

$P(n)$: « $H_{2^n} \geq 1 + \frac{n}{2}$ »

En appliquant la définition, $H_{2^n} = 1 + \frac{1}{2} + \cdots + \frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{2^n}$

<u>Cas de base :</u> $n = 0$, $H_{2^n} = H_{2^0} = H_1 = 1 \underbrace{\geq}_{\text{ici} =} 1 + \frac{0}{2}$, donc $P(0)$ est vraie

<u>Induction :</u> On suppose que $P(n)$ est vraie, et on montre $P(n+1)$.

Au rang $n + 1$

$$H_{2^{n+1}} = \underbrace{H_{2 \cdot 2^n}}_{*} = \underbrace{1 + \frac{1}{2} + \cdots + \frac{1}{2^n}}_{= H_{2^n} \quad **} + \underbrace{\frac{1}{2^n+1} + \frac{1}{2^n+2} + \cdots + \frac{1}{2^{n+1}}}_{***}$$

$*$ Il y a $2 \cdot 2^n$ termes. $**$ Il y a 2^n termes.

Dans une suite harmonique, le premier terme est le plus grand. Tous les termes suivant sont inférieurs ou égaux au premier terme.

$***$ Il y a 2^n termes et tous sont inférieurs ou égaux à $\frac{1}{2^{n+1}}$. $\frac{1}{2^{n+1}}$ est la borne inférieure de valeur de chacun des termes de ces termes.

$$H_{2^{n+1}} \geq H_{2^n} + \cancel{2^n} \cdot \frac{1}{\underbrace{2^{n+1}}_{2 \cdot \cancel{2^n}}}$$

$$H_{2^{n+1}} \geq H_{2^n} + \frac{1}{2}$$

$H_{2^{n+1}} \geq 1 + \frac{n}{2} + \frac{1}{2}$

(hypothèse d'induction)

$H_{2^{n+1}} \geq 1 + \frac{n+1}{2}$

2. Montrer par induction que $H_n = \frac{p_n}{q_n}$ avec p_n entier positif impair et q_n entier positif pair pour $n \geq 2$. En déduire que H_n n'est pas entier pour $n \geq 2$.

$$H_n = \frac{p_n > 0 \ \text{impair}}{q_n > 0 \ \text{pair}}$$

H_n est une fraction donc $H_n \notin \mathbb{Z}$ pour $n \geq 2$.

Cas de base : $n = 2$,

$$H_2 = \frac{3\ (p_2)}{2\ (q_2)}$$

donc $P(2)$ est vraie

Induction généralisée : On suppose que $\forall k \leq n$, $P(k)$ soit vraie, et on montre $P(n+1)$.

$$H_{n+1} = H_n + \frac{1}{n+1} = \frac{p_n}{q_n} + \frac{1}{n+1} = \frac{p_n(n+1) + q_n}{q_n(n+1)}$$

hypothèse d'induction $H_n = \frac{p_n}{q_n}$

Rappel : parité

pair + pair = pair pair + impair = impair impair + impair = pair	pair × pair = pair pair × impair = pair impair × impair = impair

1) si $n+1$ impair

$$H_{n+1} = \frac{p_n(n+1) + q_n}{q_n(n+1)} = \frac{I \cdot I + P}{P \cdot I} = \frac{I}{P}$$

↑ informellement

2) si $n+1$ pair

$$H_{n+1} = \frac{p_n(n+1) + q_n}{q_n(n+1)} = \frac{I \cdot P + P}{P \cdot P}$$

On manipule H_{n+1} pour obtenir ce qu'on veut. On sépare les termes dont le dénominateur est impair des termes dont le dénominateur est pair.

$$H_{n+1} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \frac{1}{n+1}$$

$$H_{n+1} = \underbrace{1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2k-1}}_{\text{dénominateur impair}} + \underbrace{\frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \cdots + \frac{1}{2k}}_{\text{dénominateur pair}}$$

$$H_{n+1} = \left(1 + \frac{1}{3} + \cdots + \frac{1}{2k-1}\right) + \frac{1}{2}\underbrace{\left(1 + \frac{1}{3} + \cdots + \frac{1}{k}\right)}_{H_k}$$

On se rend compte qu'il s'agit d'une induction généralisée. Au lieu de supposer que $P(n)$ est vraie, on suppose que $P(k)$ est vraie pour tout $k \leq n$.

$$H_k = \frac{p_k}{q_k} \quad \text{avec } k < n$$

$$H_{n+1} = \frac{1}{2} \cdot \frac{p_k}{q_k} + \left(1 + \frac{1}{3} + \cdots + \frac{1}{2k-1}\right)$$

$$H_{n+1} = \frac{p_k}{2q_k} + \frac{a}{b}$$

$$\frac{a}{b} = \frac{a}{\underbrace{1 \cdot 3 \cdot 5 \cdot 7 \cdots (2k-1)}_{\text{produit des nombres impairs}}}$$

$$H_{n+1} = \frac{p_k \cdot b + 2q_k \cdot a}{2q_k \cdot b} = \frac{I}{P}$$

Exercice 4

On rappelle que les nombres de Fibonacci sont définis par $F_n = F_{n-1} + F_{n-2}$ pour $n > 1$ et $F_0 = 0$, $F_1 = 1$.

Montrer que pour tout $n > 0$:

1. $F_1 + F_3 + \cdots + F_{2n-1} = F_{2n}$

Cas de base : $n = 1$, $F_1 = F_2$ (car $1 = 1$), $P(1)$ est vraie

Induction : $P(n)$ est vraie, on montre $P(n+1)$.

$P(n+1)$: on veut avoir $F_1 + F_3 + \cdots + \underbrace{F_{2(n+1)-1}}_{F_{2n+1}} = F_{2(n+1)}$

$$F_{2(n+1)} = F_{2n+2} \underbrace{=}_{*} F_{2n} + F_{2n+1}$$

par hypothèse d'induction ↓ $\quad$ $*$ par définition de la suite de Fibonacci

$$F_{2(n+1)} = F_1 + F_3 + \cdots + F_{2n-1} + \underbrace{F_{2n+1}}_{*}$$

$*$ le terme suivant d'indice impair

2. $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$

Cas de base : $n = 1$, $\underbrace{F_2}_{1} \cdot \underbrace{F_0}_{0} - \underbrace{F_1^2}_{1} = 0 - 1^2 = -1 = (-1)^1$

Induction : $P(n)$ vrai, et on montre $P(n+1)$

$P(n+1)$: $F_{(n+1)+1}F_{(n+1)-1} - F_{n+1}^2 = (-1)^{n+1}$

$$F_{n+2}F_n - F_{n+1}^2 = (-1)^{n+1}$$

$$F_{n+2}F_n - F_{n+1}^2 = (F_n + F_{n+1})F_n - F_{n+1}^2$$

(par définition de la suite de Fibonacci)

$$= F_n^2 + F_n \cdot F_{n+1} - F_{n+1}^2$$

$$= F_n^2 + F_{n+1}(F_n - F_{n+1})$$

Par définition de Fibonacci, $F_{n+1} = F_{n-1} + F_n \Rightarrow F_n - F_{n+1} = -F_{n-1}$

$$= F_n^2 + F_{n+1}(-F_{n-1})$$
$$= -F_{n+1} \cdot F_{n-1} + F_n^2$$
$$= -1\,\underbrace{(F_{n+1}F_{n-1} - F_n^2)}_{(-1)^n}$$

→ par hypothèse d'induction

Par hypothèse d'induction, $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$

Au rang $n+1$, c'est égal à $(-1)^1 \cdot (-1)^n = (-1)^{n+1}$

3. $F_1^2 + F_2^2 + \cdots + F_n^2 = F_nF_{n+1}$

<u>Cas de base :</u> $n = 1$, $F_1^2 = 1 = \underbrace{F_1}_{1} \cdot \underbrace{F_2}_{1}$

<u>Induction :</u> $P(n+1) : F_{n+1}\underbrace{F_{n+2}}_{*} = F_{n+1}(F_n + F_{n+1})$

$*$ par définition de Fibonacci, $F_{n+2} = F_n + F_{n+1}$

$F_{n+1}F_{n+2} = F_nF_{n+1} + F_{n+1}^2$

par hypothèse d'induction ↓

$F_{n+1}F_{n+2} = F_1^2 + F_2^2 + \cdots + F_n^2 + F_{n+1}^2$

4. F_{3n} est pair.

<u>Cas de base :</u> $n = 1$, $F_{3\cdot 1} = 2$, donc $P(1)$ vraie

<u>Induction :</u> On suppose que F_{3n} est pair, on montre que $F_{3(n+1)} = F_{3n+3}$ est pair.

On applique successivement la définition de Fibonacci.

$F_{3n+3} = F_{3n+1} + F_{3n+2}$

$F_{3n+3} = F_{3n+1} + F_{3n} + F_{3n+1}$

$F_{3n+3} = F_{3n} + 2 \cdot F_{3n+1}$

F_{3n} est pair par hypothèse d'induction.

$2 \cdot F_{3n+1}$ est pair car de la forme $2k$.

donc F_{3n+3} est pair.

<u>Conclusion :</u> Avec le cas de base $P(1)$ et l'induction $P(n+1)$, on a montré que pour tout $n > 0$, F_{3n} est pair.

(La conclusion est une phrase type à réutiliser à la fin de chaque démonstration par induction.)

5. $\varphi^{n-2} \leq F_n \leq \varphi^{n-1}$, où $\varphi = \frac{1+\sqrt{5}}{2}$ est la solution positive de $r^2 - r - 1 = 0$.

Suite de Fibonacci

Géométriquement : a et b sont deux segments contigus.

$$\frac{a}{b} = \frac{a+b}{a}$$

On peut trouver le terme général d'une suite définie par récurrence en résolvant son équation associée.

Pour la suite de Fibonacci, l'équation est $r^2 - r - 1 = 0$.
Cette équation à deux racines :

$$r_1 = \varphi, r_2 = \frac{1-\sqrt{5}}{2}$$

Donc le terme général de la suite de Fibonacci est :

$$F_n = \alpha \cdot r_1^n + \beta \cdot r_2^n$$
$$\alpha = \frac{1}{\sqrt{5}}, \beta = -\frac{1}{\sqrt{5}}$$

Induction forte

Cas de base : $n = 1$, et $n = 2$

$$\varphi^{-1} \leq F_1 \leq \varphi^0 \Leftrightarrow \underbrace{\frac{2}{1+\underbrace{\sqrt{5}}_{>2}}}_{\leq 1} \leq 1 \leq 1 \qquad \left(\varphi^{-1} = \frac{1}{\varphi} = \frac{2}{1+\sqrt{5}}\right)$$

$$\varphi^0 \leq F_2 \leq \varphi^1 \Leftrightarrow 1 \leq 1 \leq \underbrace{\frac{\overbrace{1+\sqrt{5}}^{>3}}{2}}_{\geq 1}$$

Induction générale : On suppose que $\forall k \leq n$, $P(k)$ est vraie.

Au rang $n+1$, $F_{n+1} = F_{n-1} + F_n$

Majoration de F_{n+1} :

$F_{n+1} = F_{n-1} + F_n$

Par hypothèse d'induction, $F_{n-1} \leq \underbrace{\varphi^{(n-1)-1}}_{\varphi^{n-2}}$ et $F_n \leq \varphi^{n-1}$.

$F_{n+1} \leq \varphi^{n-2} + \varphi^{n-1}$

$F_{n+1} \leq \varphi^{n-2}(1+\varphi)$

φ est la solution de $\varphi^2 - \varphi - 1 = 0 \Rightarrow \varphi^2 = \varphi + 1$

$F_{n+1} \leq \varphi^{n-2} \cdot \varphi^2$

$F_{n+1} \leq \varphi^n \Leftrightarrow F_{n+1} \leq \varphi^{(n+1)-1}$

Minoration de F_{n+1} :

$F_{n+1} = F_{n-1} + F_n$

Par hypothèse d'induction, $F_{n-1} \geq \underbrace{\varphi^{(n-1)-2}}_{\varphi^{n-3}}$ et $F_n \geq \varphi^{n-2}$.

$F_{n+1} \geq \varphi^{n-3} + \varphi^{n-2}$

$F_{n+1} \geq \varphi^{n-3}(1+\varphi)$

même raisonnement que pour la majoration de F_{n+1}

$F_{n+1} \geq \varphi^{n-3} \cdot \varphi^2$

$F_{n+1} \geq \varphi^{n-1} \Leftrightarrow F_{n+1} \geq \varphi^{(n+1)-2}$

Donc $\varphi^{(n+1)-2} \leq F_{n+1} \leq \varphi^{(n+1)-1}$

Exercice 5

Donner une définition inductive de $f(n) = a^{2^n}$.

Indication : On pourra remarquer que $a^{2^{n+1}} = \left(a^{2^n}\right)^2$ car $2^{n+1} = 2 \cdot 2^n$

$a^{2^{n+1}} = a^{2^n \cdot 2} \underbrace{=}_{*} a^{2^n + 2^n} = a^{2^n} \cdot a^{2^n} = \left(a^{2^n}\right)^2$

$*$ On décompose en somme.

On a exprimé le rang $n+1$ en fonction de n. Le travail était déjà fait car l'énoncé nous donnait $a^{2^{n+1}} = \left(a^{2^n}\right)^2$.

$$f(n) = \begin{cases} f(0) = a^{2^0} = a^1 = a, \quad \text{pour } n = 0 \\ \underbrace{f(n+1)}_{a^{2^{n+1}}} = \underbrace{\left(f(n)\right)^2}_{a^{2^n}} \end{cases}$$

Exercice 6

On considère le polynôme à coefficients réels $P(x) = \frac{1}{3}x^3 + ax^2 + bx$.

1. Trouver a et b pour que $\forall x \in \mathbb{R}$, $P(x+1) - P(x) = x^2$. On suppose dans la suite que cette propriété est vérifiée.

$$P(x+1) = \frac{1}{3}(x+1)^3 + a(x+1)^2 + b(x+1)$$

$$P(x+1) = \frac{1}{3}(x^3 + 3x^2 + 3x + 1) + a(x^2 + 2x + 1) + b(x+1)$$

$$P(x+1) = \frac{1}{3}x^3 + x^2 + x + \frac{1}{3} + ax^2 + 2ax + a + bx + b$$

$$P(x+1) - P(x) = \frac{1}{3}x^3 + x^2 + x + \frac{1}{3} + ax^2 + 2ax + a + bx + b - \frac{1}{3}x^3 - ax^2 - bx$$

$$P(x+1) - P(x) = x^2 + x + 2ax + a + b + \frac{1}{3}$$

$$P(x+1) - P(x) = x^2 + (2a+1)x + \left(a + b + \frac{1}{3}\right)$$

$$x^2 + (2a+1)x + \left(a + b + \frac{1}{3}\right) = x^2$$

Cette équation est vraie seulement si les coefficients autre que celui de x^2 sont nuls.

$$2a + 1 = 0 \Rightarrow a = -\frac{1}{2}$$

$$a + b + \frac{1}{3} = 0 \Rightarrow -\frac{1}{2} + b + \frac{1}{3} = 0 \Rightarrow b = \frac{1}{6}$$

2. Montrer que pour tout $n \in \mathbb{N}$, $P(n)$ est un entier.

$Q(N)$: « $P(n)$ est un entier », pour $n \in \mathbb{N}$

<u>Cas de base :</u> $Q(0)$ est vraie car $P(0) = 0$ pour $n = 0$.

Induction : On suppose $Q(n)$ vraie, on montre $Q(n+1)$.

On suppose que $P(n) \in \mathbb{N}$, et on montre que $P(n+1) \in \mathbb{N}$.

$P(n+1) = P(n) + n^2$ (d'après la proposition $P(x+1) - P(x) = x^2$ démontrée dans Q1)

Par hypothèse d'induction, $P(n) \in \mathbb{N}$ et $n^2 \in \mathbb{N}$, donc $P(n+1) \in \mathbb{N}$.

3. Pour tout $n \geq 0$, on pose $S_n = \sum_{k=0}^{n} k^2$. Montrer que

$$\forall n \geq 0, S_n = P(n+1) = \frac{n(n+1)(2n+1)}{6}$$

Cas de base : $n = 0$

$S_0 = 0^2 = 0$

$$P\underbrace{(0+1)}_{1} = \frac{1}{3} - \frac{1}{2} + \frac{1}{6} = 0$$

Donc $S_0 = P(0+1)$.

Induction : On suppose que $S_n = P(n+1)$ et on montre que $S_{n+1} = P\big((n+1)+1\big)$.

$S_{n+1} = S_n + (n+1)^2$

$S_{n+1} = P(n+1) + (n+1)^2$ par hypothèse d'induction

D'après la question 1, $P(x+1) - P(x) = x^2$.

Pour $x = n+1$, $P\big((n+1)+1\big) - P(n+1) = (n+1)^2$

soit $P(n+1) + (n+1)^2 = P\big((n+1)+1\big)$. Donc :

$S_{n+1} = P\big((n+1)+1\big)$

Exercice 7

1. On suppose qu'une propriété P définie sur $\mathbb{N}$ vérifie :
   (a) $P(1)$ est vraie
   (b) si $P(n)$ est vraie alors $P(2n)$ est vraie (pour $n \geq 1$)
   (c) si $P(n)$ est vraie alors $P(n-1)$ est vraie (pour $n \geq 2$)
   Montrer par récurrence sur n que $P(n)$ est vraie pour tout $n \geq 1$.

Par récurrence (induction) sur $\mathbb{N}$.

Cas de base : $n = 1$, $P(1)$ est vraie par (a).

Induction : On suppose que $P(n)$ est vraie.

Alors par (b) on a $P(2n)$ est vraie.

Puis par (c) on sait que $P(2n-1), P(2n-2), \cdots, P(n+1)$ sont vraies (en appliquant itérativement/successivement (c)) car $2n-1, 2n-2, \cdots, n+1$ sont tous ≥ 2.

Donc, en supposant $P(n)$ on montre que $P(n+1)$ est vraie.

Conclusion : Donc, $P(n)$ est vraie $\forall n \geq 1$.

2. On veut montrer que la moyenne arithmétique est supérieure à la moyenne géométrique. Soient $a_1, \cdots, a_n$ n nombres réels positifs, avec $n \geq 1$; on pose $A = (a_1 + \cdots + a_n)/n$ et $G = (a_1, \cdots, a_n)^{1/n}$.

$$A = \frac{a_1 + \cdots + a_n}{n} \qquad G = \sqrt[n]{a_1 \cdots a_n} = (a_1 \cdots a_n)^{1/n}$$

Cas de base : $n = 1$, on a uniquement 1 élément a_1, donc $A = G = a_1 \Rightarrow$ inutile pour le raisonnement

$n = 2, A = \dfrac{a_1 + a_2}{2}$ et $G = \sqrt{a_1 a_2}$

A-t-on $A \geq G$ (i.e. $\frac{a_1+a_2}{2} \geq \sqrt{a_1 a_2}$) ? oui

Astuce : Utiliser $(x + y)^2 = x^2 + 2xy + y^2$

Effectivement, $\underbrace{(\sqrt{a_1} - \sqrt{a_2})^2}_{\geq 0\ *} = \underbrace{\sqrt{a_1}^2}_{a_1} - 2\underbrace{\sqrt{a_1}\sqrt{a_2}}_{\sqrt{a_1 a_2}} + \underbrace{\sqrt{a_2}^2}_{a_2} = a_1 - \underbrace{2\sqrt{a_1 a_2}}_{\geq 0\ **} + a_2$

$*$ car c'est un nombre au carré

$**$ car c'est une racine carrée multipliée par un nombre positif

D'après l'énoncé, a_1 et a_2 sont des nombres réels positifs donc $a_1 - 2\sqrt{a_1 a_2} + a_2 \geq 0$

d'où $a_1 + a_2 \geq 2\sqrt{a_1 a_2}$ (on divise les deux membres par 2)

$$\Leftrightarrow \underbrace{\frac{a_1 + a_2}{2}}_{A_2} \geq \underbrace{\sqrt{a_1 a_2}}_{G_2}$$

Induction : On suppose que $P(n)$ est vraie, i.e. que pour n entiers, $A_n \geq G_n$ et on montre 2 implications :

(1) $P(n) \Rightarrow P(2n)$
(2) $P(n) \Rightarrow P(n-1)$

$\rightarrow$ d'où le résultat final $P(n)$ vraie pour tout n

(1) $P(2n) : A_{2n} \geq G_{2n}$?

$$A_{2n} = \frac{a_1 + a_2 + \cdots + a_n + a_{n+1} + \cdots + a_{2n}}{2n}$$

$$= \frac{1}{2}\left(\overbrace{\underbrace{\frac{a_1 + a_2 + \cdots + a_n}{n}}_{n \text{ éléments}}}^{A_n} + \overbrace{\underbrace{\frac{a_{n+1} + \cdots + a_{2n}}{n}}_{n \text{ éléments}}}^{A_n}\right)$$

On peut appliquer l'hypothèse d'induction à chaque « paquet » de n éléments :

$$= \frac{1}{2}\left(\frac{a_1 + a_2 + \cdots + a_n}{n} + \frac{a_{n+1} + \cdots + a_{2n}}{n}\right) \geq \frac{1}{2}\left(\underbrace{(a_1 \cdots a_n)^{1/n}}_{G_n = x} + \underbrace{(a_{n+1} \cdots a_{2n})^{1/n}}_{G_n = y}\right)$$

Par $P(2)$, $\frac{x+y}{2} \geq \sqrt{xy}$ $\quad (\sqrt{xy} = (xy)^{1/2})$

et donc $A_{2n} \geq \left((a_1 \cdots a_n)^{1/n} \cdot (a_{n+1} \cdots a_{2n})^{1/n}\right)^{1/2}$

$A_{2n} \geq (a_1 \cdots a_{2n})^{1/n \cdot 1/2}$

$A_{2n} \geq \underbrace{(a_1 \cdots a_{2n})^{1/2n}}_{G_{2n}}$

(2) $P(n) \Rightarrow P(n-1)$

$P(n-1) : A_{n-1} \geq G_{n-1}$?

Pour $n - 1$ nombres donnés $a_1, a_2, \cdots, a_{n-1}$, on choisit le n-ième nombre

$a_n = \dfrac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}$ et on utilise $P(n)$ avec ce nouvel ensemble de nombres.

L'astuce réside dans le fait de choisir judicieusement a_n, de manière à simplifier nos calculs. a_n est la moyenne arithmétique des $n - 1$ premiers éléments.

On a : $A_{n-1} = \dfrac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} = a_n$

et $A_n = \dfrac{a_1 + a_2 + \cdots + a_{n-1} + a_n}{n} = \dfrac{a_1 + a_2 + \cdots + a_{n-1} + \dfrac{a_1 + a_2 + \cdots + a_{n-1}}{n-1}}{n}$

Pour faire passer $n-1$ du numérateur au dénominateur, on multiplie le numérateur et le dénominateur par $n-1$:

$$A_n = \frac{(n-1)(a_1 + a_2 + \cdots + a_{n-1}) + (a_1 + a_2 + \cdots + a_{n-1}) \times 1}{n(n-1)}$$

On factorise par $(a_1 + a_2 + \cdots + a_{n-1})$:

$$A_n = \frac{n(a_1 + a_2 + \cdots + a_{n-1})}{n(n-1)} = \frac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} = A_{n-1} = a_n$$

d'où $A_n = \dfrac{a_1 + a_2 + \cdots + a_n}{n} = \dfrac{a_1 + a_2 + \cdots + a_{n-1}}{n-1} = a_n = A_{n-1}$

Par $P(n)$, $A_n \geq G_n$ (hypothèse d'induction),

donc $A_n \geq (a_1 \cdots a_n)^{1/n} \Leftrightarrow A_n \geq (a_1 \cdots a_{n-1})^{1/n} \cdot \underbrace{a_n^{1/n}}_{A_n}$

et on divise tout par $A_n^{1/n}$

Donc $A_n^{1-1/n} \geq (a_1 \cdots a_{n-1})^{1/n} \Leftrightarrow A_n^{(n-1)/n} \geq (a_1 \cdots a_{n-1})^{1/n}$

et en élevant tout à la puissance $n/(n-1)$, on obtient

$$\left(A_n^{(n-1)/n}\right)^{n/(n-1)} \geq (a_1 \cdots a_{n-1})^{1/n \cdot n/(n-1)}$$

$$\Leftrightarrow \underbrace{A_n}_{A_{n-1}} \geq \underbrace{(a_1 \cdots a_{n-1})^{1/(n-1)}}_{G_{n-1}}$$

TD 4 : Induction structurelle

Exercice 1. Relations définies inductivement

1. On définit inductivement l'ensemble $\mathrm{Inf}_1 \subseteq \mathbb{N} \times \mathbb{N}$ par :
   - (R_{11}) : pour tout $n \in \mathbb{N}$, $(0, n) \in \mathrm{Inf}_1$
   - (R_{12}) : pour tous $n_1, n_2 \in \mathbb{N}$, si $(n_1, n_2) \in \mathrm{Inf}_1$, alors $(n_1 + 1, n_2 + 1) \in \mathrm{Inf}_1$

   (a) Donner quelques éléments de l'ensemble Inf_1 et en déduire une propriété sur n_1 et n_2 lorsque $(n_1, n_2) \in \mathrm{Inf}_1$.

Éléments de Inf_1

$(0,0), (0,1), (0,2), \cdots, (R_{11})$

$(1,1), (1,2), (1,3), \cdots, (R_{12}) \cup (2,2), (2,3), (2,4), \cdots$

Éléments de Inf_1 : toute paire d'entiers (n_1, n_2) telle que $n_1 \leq n_2$

   (b) Montrer que pour tout $n \in \mathbb{N}$, $(n, n) \in \mathrm{Inf}_1$

Par récurrence sur n.

Cas de base : $n = 0$, on a bien $(0,0) \in \mathrm{Inf}_1$, d'après R_{11}

Induction : On suppose que $(n, n) \in \mathrm{Inf}_1$, et montrons que $(n + 1, n + 1) \in \mathrm{Inf}_1$.

D'après R_{12}, on obtient le résultat directement $(n_1 = n_2 = n)$.

   (c) Montrer que pour tous $n_1, n_2 \in \mathbb{N}$, si $(n_1, n_2) \in \mathrm{Inf}_1$, alors $(n_1, n_2 + 1) \in \mathrm{Inf}_1$.

$$\rightarrow P\big((n_1, n_2)\big)$$

Par induction sur (n_1, n_2).

Cas de base : $P\big((0, n)\big) \Rightarrow P\big((0, n + 1)\big)$

$(n_1, n_2) = (0, n)$, et d'après R_{11}, on a bien $(0, n + 1) \in \mathrm{Inf}_1$.

Induction :

On suppose que $P\big((n_1, n_2)\big)$ est vraie, et on montre que $P\big((n_1 + 1, n_2 + 1)\big)$ est vraie

i.e. on suppose que $(n_1, n_2 + 1) \in \mathrm{Inf}_1$ (hypothèse d'induction), et on montre que $(n_1 + 1, n_2 + 1 + 1) \in \mathrm{Inf}_1$.

Par hypothèse, et d'après R_{12}, on a bien $(n_1 + 1, n_2 + 1 + 1) \in \mathrm{Inf}_1$.

Par hypothèse d'induction, si $(n_1, n_2) \in \mathrm{Inf}_1$, alors $(n_1, n_2 + 1) \in \mathrm{Inf}_1$. D'après R_{12}, comme $(n_1, n_2 + 1) \in \mathrm{Inf}_1$, $(n_1 + 1, n_2 + 1 + 1) \in \mathrm{Inf}_1$.

2. On définit inductivement l'ensemble $\mathrm{Inf}_2 \subseteq \mathbb{N} \times \mathbb{N}$ par :
   - (R_{21}) : pour tout $n \in \mathbb{N}$, $(n, n) \in \mathrm{Inf}_2$
   - (R_{22}) : pour tous $n_1, n_2 \in \mathbb{N}$, si $(n_1, n_2) \in \mathrm{Inf}_2$, alors $(n_1, n_2 + 1) \in \mathrm{Inf}_2$

   (a) Donner quelques éléments de l'ensemble Inf_2 et en déduire une propriété sur n_1 et n_2 lorsque $(n_1, n_2) \in \mathrm{Inf}_2$.

   (b) Montrer que pour tout $n \in \mathbb{N}, (0, n) \in \mathrm{Inf}_2$.

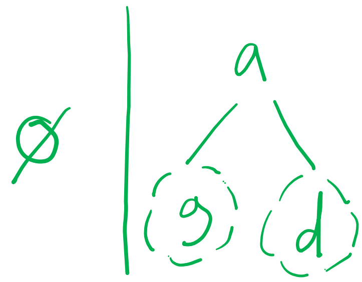
   (c) Montrer que pour tous $n_1, n_2 \in \mathbb{N}$, si $(n_1, n_2) \in \mathrm{Inf}_2$ alors $(n_1 + 1, n_2 + 1) \in \mathrm{Inf}_2$.

Exercice 2. Arbres binaires

Rappel : Définition inductive d'un arbre binaire

Arbres binaires étiquetés (AB)

$$\begin{cases} (B) & \emptyset \in AB \\ (I) & \text{si } g, d \in AB, \text{alors } \forall a \in \text{alphabet } A, (a, g, d) \in AB \end{cases}$$



On considère l'ensemble AB des arbres binaires (0, 1 ou 2 fils par nœud) sur un alphabet A.

1. Donner une définition inductive de la hauteur $h(t)$, du nombre de nœuds $n(t)$, du nombre de d'arrêtes $ar(t)$ et du nombre de feuilles $f(t)$ d'un arbre binaire.

t, pour *tree* en anglais, est la notation usuelle pour un arbre binaire.

Cas de base : $t = \emptyset$

$h(t) = h(\emptyset) = 0$

$n(t) = n(\emptyset) = 0$

$ar(t) = ar(\emptyset) = 0$

$f(t) = f(\emptyset) = 0$

Induction : $t = (a, g, d)$

$h(t) = 1 + \max\big(h(g), h(t)\big)$

$n(t) = 1 + n(g) + n(d)$

$$ar(t) = \begin{cases} 0 \text{ si } g = d = \emptyset \\ 1 + ar(g) \text{ si } d = \emptyset \\ 1 + ar(d) \text{si } g = \emptyset \\ 2 + ar(g) + ar(t) \text{ si } g \; et \; d \neq \emptyset \end{cases}$$

$$f(t) = \begin{cases} 1 \text{ si } g = d = \emptyset \\ f(g) + f(t) \text{ si } g \text{ ou } d \neq \emptyset \end{cases}$$

2. Montrer que pour tout arbre t de AB, $n(t) \leq 2^{h(t)} - 1$, et que $f(t) \leq 2^{h(t)-1}$.

$P(t) : n(t) \leq 2^{h(t)} - 1$ $\qquad$ $Q(t) : f(t) \leq 2^{h(t)-1}$

Preuves par induction structurelle sur AB.

$P(t)$ Cas de base : L'unique élément de la base est l'arbre vide $\emptyset$,

et $n(\emptyset) = 0 = 2^{\overbrace{h(\emptyset)}^{=0}} - 1 = 2^0 - 1 = 1 - 1 = 0$

Induction : On suppose que $P(g)$ et $P(d)$ et on montre $P\big((a, g, d)\big)$

sous-arbre gauche $\qquad$ sous-arbre droit $\qquad$ t

$n(t) \underbrace{=}_{*} 1 + n(g) + n(d) \leq 1 + 2^{h(g)} - 1 + 2^{h(d)} - 1$ $\qquad$ hypothèse d'induction

définition inductive de $n(t)$

Avec des valeurs numériques, $2^6 + 2^8 \leq 2^8 + 2^8 = 2 \cdot 2^8$.

$n(t) \leq 2 \cdot 2^{\max\left(h(g), h(d)\right)} - 1$

$n(t) \leq 2^{1+\max\left(h(g), h(d)\right)} - 1$ $\qquad$ définition inductive de $h(t)$

$n(t) \leq 2^{h(t)} - 1$

Conclusion : Donc $\forall t \in AB, n(t) \leq 2^{h(t)} - 1$.

$Q(t)$ Cas de base : $t = \emptyset$,

$$\underbrace{f(\emptyset)}_{0} \leq 2^{\overbrace{h(\emptyset)}^{0}-1} \Rightarrow 0 \leq \underbrace{2^{-1}}_{\frac{1}{2}}$$

$$f(t) = \begin{cases} 1 \text{ si } g = d = \emptyset \\ f(g) + f(t) \text{ si } g \text{ ou } d \neq \emptyset \end{cases}$$

Autre cas de base vu la définition de $f(t)$:

$$t = (a, \emptyset, \emptyset), \underbrace{f\big((a, \emptyset, \emptyset),\big)}_{1} \leq 2^{\overbrace{h\left((a,\emptyset,\emptyset)\right)}^{1}-1} = 2^0 = 1$$

Induction : On suppose $Q(g)$ et $Q(d)$ vraies.

$f(t) = f(g) + f(d)$ (par définition)

Par hypothèse d'induction, $f(g) \leq 2^{h(g)-1}$ et $f(d) \leq 2^{h(d)-1}$. Donc :

$f(t) \leq f(g) \leq 2^{h(g)-1} + f(d) \leq 2^{h(d)-1}$

$f(t) \leq 2 \cdot 2^{\max(h(g),h(d))-1}$

$f(t) \leq 2^{\overbrace{1+\max(h(g),h(d))}^{h(t)}-1}$

$f(t) \leq 2^{h(t)-1}$

Conclusion : Donc $\forall t \in AB$, $f(t) \leq 2^{h(t)-1}$.

3. Définir le parcours préfixe d'un arbre binaire.

$$\text{Pref}(t) = \begin{cases} \varepsilon & \text{si } t = \emptyset \\ a.\text{Pref}(g).\text{Pref}(d) & \text{si } t = (a, g, d) \end{cases}$$

Exercice 4. Définitions inductives sur A^*

Soit A^* le monoïde libre engendré par l'alphabet A.

Donner une définition inductive de A^*.

Le miroir d'un mot $u = a_1 a_2 \cdots a_n$ est le mot $\tilde{u} = a_n \cdots a_2 a_1$. Donner une définition inductive du miroir.

Définition inductive de A^* (un langage) :

(B) $\varepsilon \in A^*$ (mot vide)

(I) $\forall m \in A^*$ et $\forall a \in A$, $m.a \in A^*$

pour tout mot de A^* — pour toute lettre de A^* — règle de construction de nouveaux mots

$A^* = \{\varepsilon, a, aa, \cdots\}$

Définition inductive du miroir $\tilde{u}$:

$$\tilde{u} = \begin{cases} \varepsilon & \text{si } u = \varepsilon \\ a.\tilde{v} & \text{si } u = v.a \end{cases}$$

Exemple : $u = \text{"bonjour"} \Rightarrow \tilde{u} = \text{"ruojnob"}$

$u = \text{"bonjour"} = v_0.\text{"r"}$ où $v_0 = \text{"bonjou"}$

$\tilde{u} = \text{"r"}.\widetilde{v_0} = \text{"r"}.\text{"u"}.\widetilde{v_1} = \text{"r"}.\text{"u"}.\text{"o"}.\widetilde{v_2} = \cdots = \text{"ruojnob"}$

Exercice 5. Définition inductive sur $\boldsymbol{A}^*$ et définition équivalente

L'ordre préfixe sur A^* peut être défini de deux manières différentes :

1. Pour tous mots $u, v \in A^*$, $u \preccurlyeq_{pref}^{1} v$ s'il existe $w \in A^*$ tel que $v = uw$. R_1
   u, v et uw sont des mots. A^* est un langage.
   $\preccurlyeq_{pref}^{1}$ signifie « est un préfixe de » → relation d'ordre préfixe R_1.
2. Définition inductive : R_2
   (B) pour tout mot $v \in A^*$, $\varepsilon \preccurlyeq_{pref}^{2} v$
   (I) Si $u, v \in A^*$ sont tels que $u \preccurlyeq_{pref}^{2} v$, alors pour toute lettre $a \in A$, $au \preccurlyeq_{pref}^{2} av$
   A est un alphabet. $\preccurlyeq_{pref}^{2}$ → relation d'ordre R_2

Montrer que ces deux définitions sont équivalentes.

On montre la double inclusion : $R_1 \subseteq R_2$ et $R_2 \subseteq R_1$.
Les relations R_1 et R_2 sont des sous-ensembles de $A^* \times A^*$.
$R_1 \subseteq R_2$ On considère la propriété :
$P(u)$: $\forall v \in A^*$, si $(u, v) \in R_1$, alors $(u, v) \in R_2$
raisonnement par induction sur la longueur du mot $u = |u|$
<u>Cas de base :</u> pour $u = \varepsilon$, $|u| = |\varepsilon| = 0$
et comme $v \in A^*$, alors $(u, v) \in R_1$ car $\exists w \in A^*$ tel que $v = \varepsilon . w$ et ce w est égal à v.
Et d'après **(B)** de R_2, on sait que ε est le préfixe de tout mot de A^*, donc $P(\varepsilon)$ est vraie.
<u>Induction :</u> On suppose que P est vraie pour des mots de longueur n, et on montre P pour la longueur $n + 1$.
Donc soit $u = a.u'$ un mot de $\in A^*$ de longueur $n + 1$.
$|u| = n + 1$ et $|u'| = n$
Soit $(u, v) \in R_1$. Par définition de R_1, $\exists w \in A^*$ tel que $v = u.w$ donc $v = \boldsymbol{a}.u'.w$.
Donc le mot v commence par $\boldsymbol{a}$ et peut s'écrire $v = \boldsymbol{a}.v'$. On en déduit que $v' = u'w$.
Par définition de R_1, u' est un préfixe de v', donc $(u', v') \in R_1$. De plus, u' étant de longueur n, on applique l'hypothèse d'induction, d'où $(u', v') \in R_2$.
D'après **(I)** de R_2, on en déduit $(au', av') \in R_2$ donc $(u, v) \in R_2$.
$au' = u$ et $av' = v$ par définition
Donc $P(u)$ est vraie pour tout u.

$R_2 \subseteq R_1$ Par définition, R_2 est le plus petit ensemble satisfaisant **(B)** et **(I)**.
En montrant que R_1 vérifie **(B)** et **(I)** on obtient l'inclusion cherchée.
<u>Cas de base :</u> Comme $(\varepsilon, v) \in R_1$, $\forall v \in A^*$, **(B)** est satisfaite par R_1.
<u>Induction :</u> Soit $(u, v) \in R_1$ et $a \in A$.
Alors par définition de R_2, $\exists w \in A^*$ tel que $v = u.w$, donc $a.v = a.uw$,
ce qui donne $(au, av) \in R_1$, et R_1 satisfait **(I)**. D'où le résultat.

<u>Conclusion :</u> Donc $R_1 = R_2$.

TD 5 : Langages et automates

1 Langages

Exercice 1

1. Soit A un alphabet. Montrer que $(\mathcal{P}(A^*), \cdot\ \{\varepsilon\})$ est un monoïde.

A^* : ensemble infini des mots composés des lettres de A

$\cdot$: produit/concaténation

ε : élément neutre, mot vide

$(L_1 \cdot L_2) \cdot L_3 = L_1 \cdot (L_2 \cdot L_3) = \{u_1 u_2 u_3 \text{ tel que } u_1 \in L_1, u_2 \in L_2, u_3 \in L_3\}$

$\underbrace{L \cdot \{\varepsilon\}}_{=\{\varepsilon\} \cdot L} = \{uv \text{ tel que } u \in L, v = \varepsilon\} = \{u\varepsilon \text{ tel que } u \in L\} = L$

$L^0 = \{\varepsilon\}$ $\quad L^1 = L \cdot L^0$ $\quad L^2 = L \cdot L^1$

2. Montrer que si $(L_i)_{i \in I}$ est une famille quelconque de langages, alors

$$\left(\bigcup_{i \in I} L_i\right) \cdot L = \bigcup_{i \in I} (L_i \cdot L)$$

Un mot $u \in (\bigcup_{i \in I} L_i) \cdot L$ ssi $\exists v$ et w tels que $u = vw$ tel que $v \in \bigcup_{i \in I} L_i$ et $w \in L$

$\Leftrightarrow \exists i \in I$ tel que $v \in L_i$, $\exists w \in L$ tel que $u = vw$ {il existe un langage L_i qui contient le mot v (puisque $v \in \bigcup_{i \in I} L_i$) puis il est concaténé pour $w \in L$

$\Leftrightarrow u \in \bigcup_{i \in I} (L_i \cdot L)$

Si $v \in L_i$ et $w \in L$ alors $u = vw \in (L_i \cdot L)$ d'où u est dans l'union qui contient $(L_i \cdot L)$.

3. Montrer que $L^* = (L + \{\varepsilon\})^*$ et que $L^* = \{\varepsilon\} + L \cdot L^*$.
4. Montrer que $\emptyset^* = \{\varepsilon\}$.

Exercice 2

Soit A un alphabet contenant la lettre b. Soit $X = \{b\}$ et $Y = (A \setminus \{b\}) \cdot \{b\}^*$.

1. Décrire informellement les éléments de X^*, Y et Y^*.

X est l'ensemble des mots composés de b longueur $0 \to \infty$ (y compris le mot vide).

Y est l'ensemble des mots commençant par une lettre différente de b, suivie d'une séquence de b (y compris ε). Y contient des mots non-vides car on a forcément au moins la lettre tirée dans $A \setminus \{b\}$.

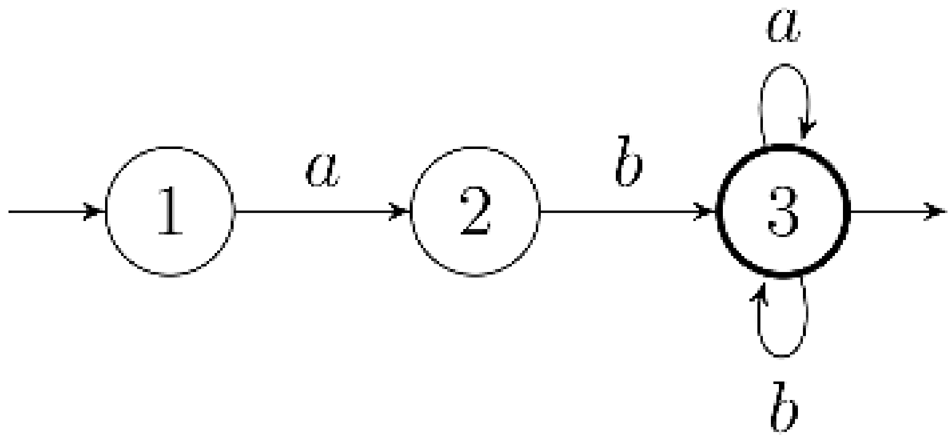
Y^* est l'ensemble des mots formé de ε et tous les mots non-vides ne commençant pas par un « b ». $\quad Y^* = \{(A \setminus \{b\}) \cdot \{b\}^*\}^*$

On sait que le mot ne commence pas par b, mais on ne sait pas ce qui se passe après avec les occurrences de b. b ne peut pas agir comme délimiteur entre les mots de Y car il peut y avoir entre 0 et un nombre infini de b à la fin d'un mot de Y.

2 Automates complets/déterministes

Exercice 3

Expliquer pourquoi l'automate suivant sur $\{a, b\}$ n'est pas complet. Quel langage reconnait-il ? Donnez un automate complet équivalent.

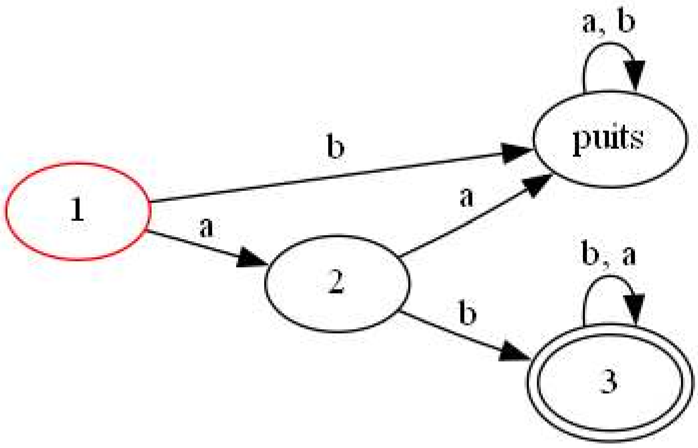


L'automate n'est pas complet car il n'existe pas de chemin partant de 1 étiqueté par b, ni de chemin partant de 2 étiqueté par a.

Langage reconnu : {mots qui comment par $ab\} = a.b.(a+b)^*$

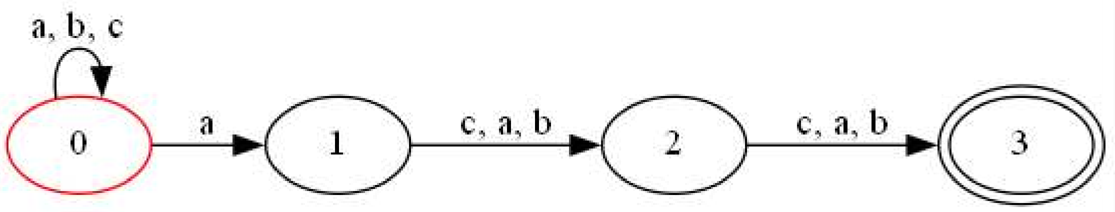
Rappel : comment compléter un automate

On ajoute un état vers lequel vont toutes les transitions manquantes. On peut entrer dans cet état, mais pas en sortir donc on l'appelle le « puits ».



Exercice 4

Représenter l'automate $\mathcal{A}$ sur l'alphabet $\{a, b, c\}$ d'états 0, 1, 2, 3, d'état initial 0, d'état terminal 3 et de transitions (0, a, 0), (0, a, 1), (0, b, 0), (0, c, 0), (1, a, 2), (1, b, 2), (1, c, 2), (2, a, 3), (2, b, 3), (2, c, 3).

$\mathcal{A}$:


1. Cet automate est-il complet ? déterministe ? justifier.

complet ? non, aucune transition ne part de l'état 3

déterministe ? non, 2 transitions (0, a, 0) et (0, a, 1)

2. Les mots $baba$ et $cabcb$ sont-ils reconnus par $\mathcal{A}$?

$baba \in L(\mathcal{A})$, $cabcb \notin L(\mathcal{A})$

Pour $cabcb$, l'exécution s'arrête au second c. Il n'y aucun moyen d'aller de c à b.

3. Décrire $L(\mathcal{A})$ en langage ordinaire.

$L(\mathcal{A})$ est l'ensemble des mots se terminant par un « a » suivi de 2 lettres.

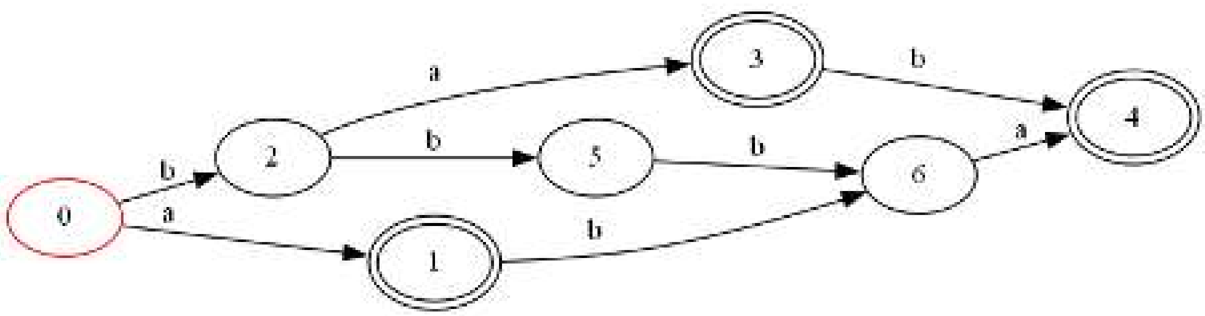
$L(\mathcal{A}) = \{a, b, c\}^*.a.\{a, b, c\}^2$

$\{a, b, c\}^*$ signifie une combinaison de longueur quelconque composée de a, de b et/ou de c.

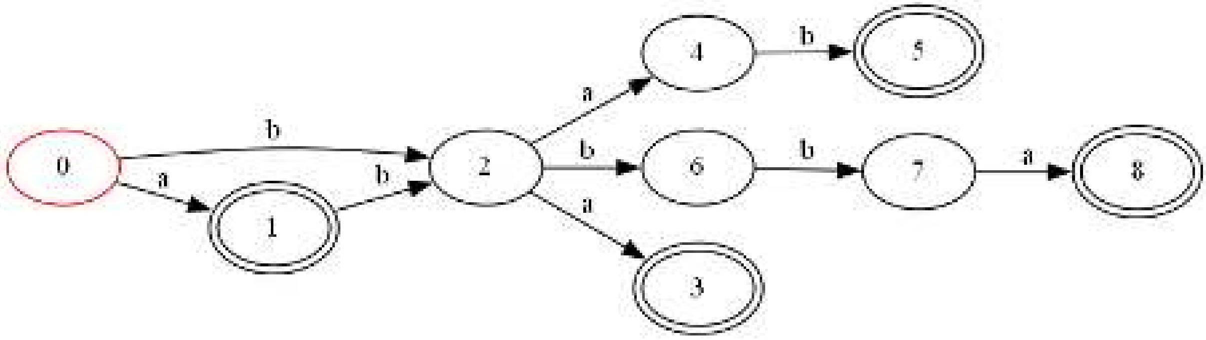
3 Construction d'automates

Exercice 5

Construire un automate déterministe reconnaissant le langage fini : $\{a, ba, aba, bab, bbba\}$.



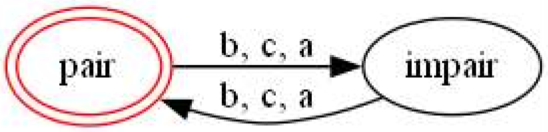
La version non déterministe est beaucoup plus simple. Il suffit de créer un chemin par mot :



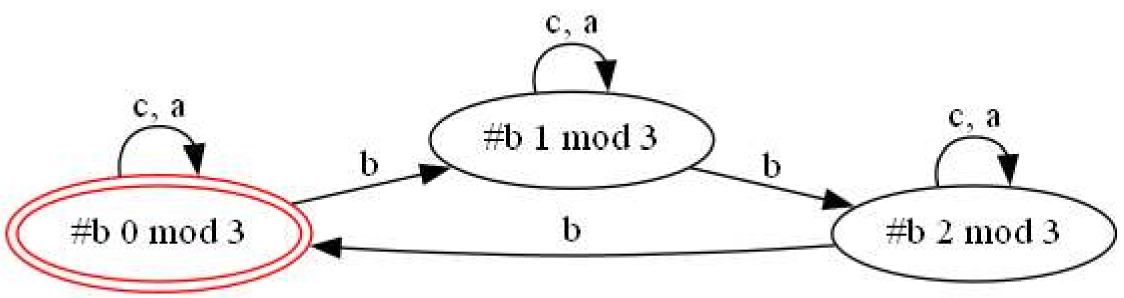
Exercice 6

Soit $A = \{a, b, c\}$. Donner des automates finis reconnaissant les langages suivants.

1. L'ensemble des mots de longueur paire.

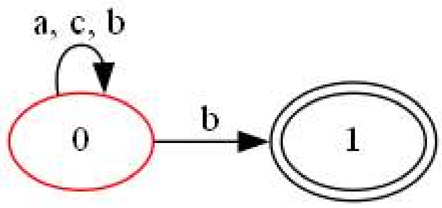


2. L'ensemble des mots où le nombre d'occurrences de « b » est divisible par 3.

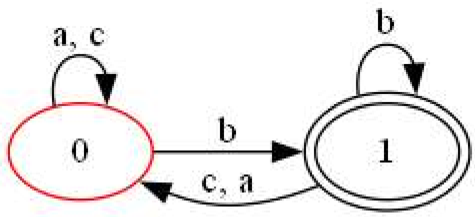


3. L'ensemble des mots se terminant par « b ».

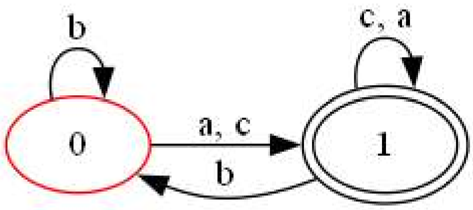
Automate ni complet ni déterministe :



Automate complet et déterministe :

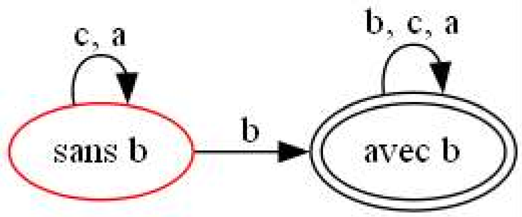


4. L'ensemble des mots non vides ne se terminant pas par « b ».



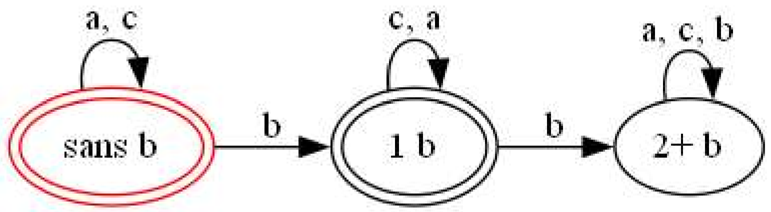
complet et déterministe

5. L'ensemble des mots contenant au moins un « b ».



complet et déterministe

6. L'ensemble des mots contenant au plus un « b ».

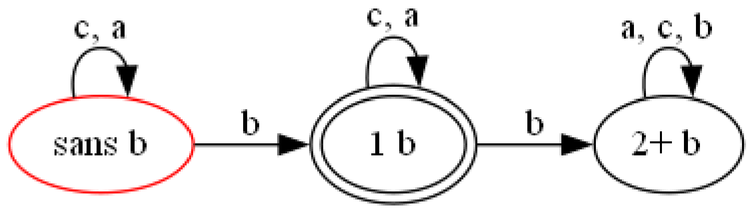


complet et déterministe

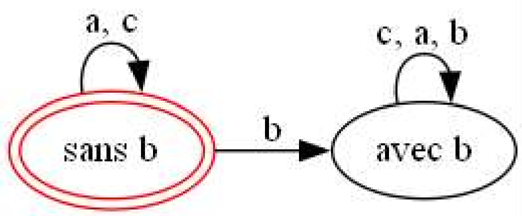
(puits)

7. L'ensemble des mots contenant exactement un « b ».

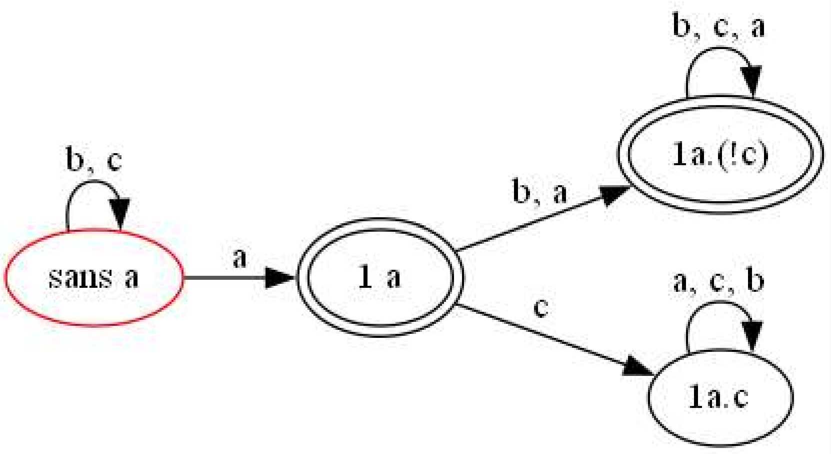
Même que la question 6 sauf que l'état « sans b » n'est plus final :



8. L'ensemble des mots ne contenant aucun « b ».



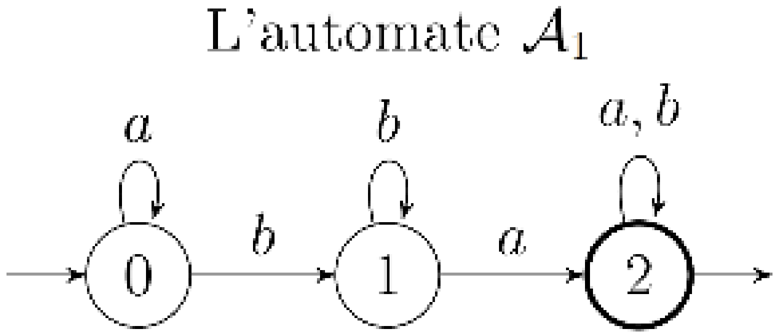
9. L'ensemble des mots contenant au moins un « a ». et dont la première occurrence de « a ». n'est pas suivie par un « c ».

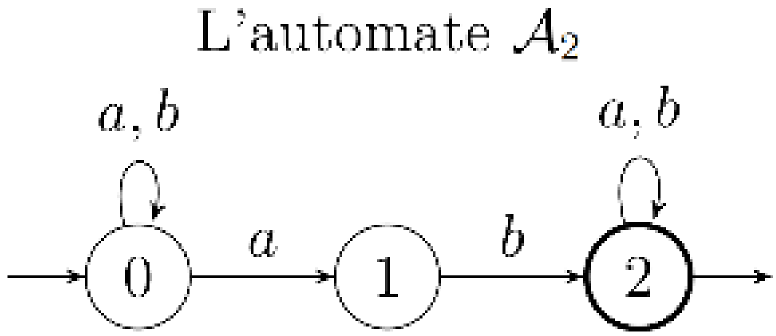


4 Opérations

Exercice 7. Intersection et déterminisation

On considère les automates $\mathcal{A}_1$ et $\mathcal{A}_2$ suivants sur l'alphabet $\{a, b\}$.





1. Construire à partir de $\mathcal{A}_1$ et $\mathcal{A}_2$ un automate acceptant l'intersection $\mathcal{L}(\mathcal{A}_1) \cap \mathcal{L}(\mathcal{A}_2)$.

Rappel : construire l'intersection de deux automates

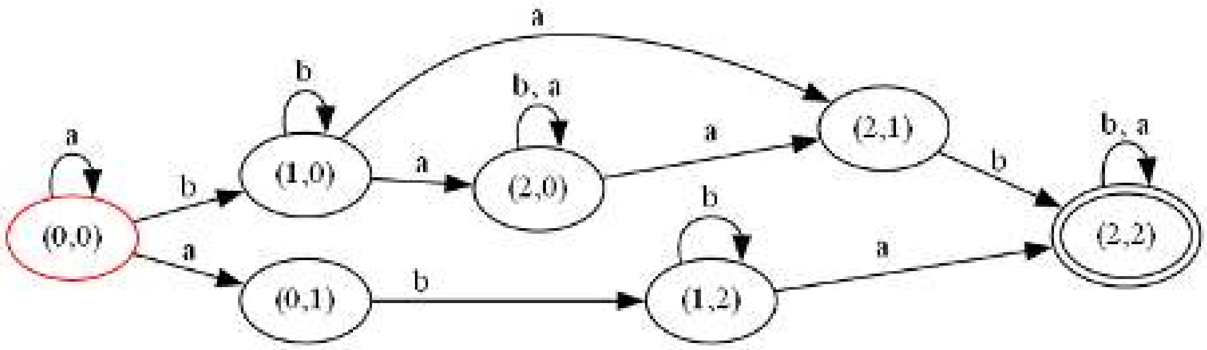
Les états initiaux sont le produit cartésien des états initiaux des deux automates.

Les états finaux sont le produit cartésien des états initiaux des deux automates.

Les transitions T_n : $\big((s_1, s_2), a, (s_1', s_2')\big) \in T_n$ ssi $(s_1, a, s_1') \in T_1$ et $(s_2, a, s_2') \in T_2$

L'intersection préserve le déterministe.

Chaque état de l'automate acceptant l'intersection $\mathcal{L}(\mathcal{A}_1) \cap \mathcal{L}(\mathcal{A}_2)$ est un couple dont le premier élément est un état de $\mathcal{A}_1$ et le second élément est un état de $\mathcal{A}_2$.



2. Les automates $\mathcal{A}_1$ et $\mathcal{A}_2$ sont-ils déterministes ? Expliquez pourquoi et si ce n'est pas le cas, déterminisez-les.

$\mathcal{A}_1$ est complet et déterministe. $\mathcal{A}_2$ n'est ni l'un ni l'autre.

Rappel : déterminiser un automate

Soit $\mathcal{P}$ l'ensemble des parties de l'ensembles des états de l'automate. On fait un tableau à deux entrées : la première colonne contient des parties de $\mathcal{P}$ et on rajoute une colonne par nouvelle étiquette de transition.

Le premier élément de la première colonne est l'ensemble des états initiaux. Cet ensemble est l'**état initial** de l'automate déterminisé.

Pour chaque élément de la première colonne (état de départ), on regarde vers quels états on peut aller par chaque étiquette (on obtient un ensemble d'états d'arrivées par étiquette) et on complète ainsi la ligne.

Dès qu'on trouve une nouvelle partie de $\mathcal{P}$, on l'ajoute à la fin de la première colonne et il faudra l'étudier.

Un ensemble de la première colonne est un **état final** de l'automate déterminisé s'il contient un état final de l'automate d'origine.

Les ensembles de la première colonne sont les états de l'automate déterminisé.

Chaque case du tableau c, sauf celles de la première colonne, correspond à la **transition** : (case de la première colonne sur la même ligne que c, étiquette de la colonne de c, c).

On déterminise $\mathcal{A}_2$:

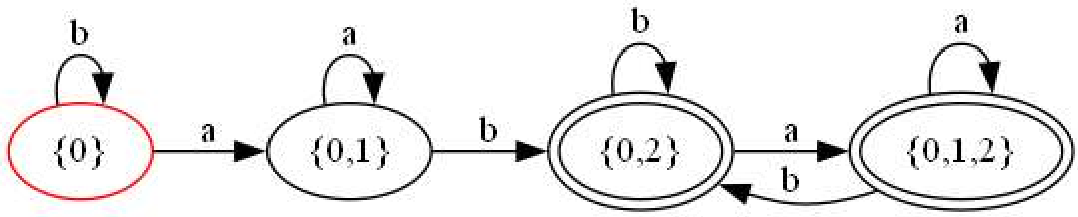
init	a	b
$\{0\}$	$\{0,1\}$	$\{0\}$
$\{0,1\}$	$\{0,1\}$	$\{0,2\}$
$\{0,2\}$	$\{0,1,2\}$	$\{0,2\}$
$\{0,1,2\}$	$\{0,1,2\}$	$\{0,2\}$

0 est initial dans $\mathcal{A}_2$ non déterministe.

a et b sont les étiquettes des transitions.

On ajoute chaque nouvel ensemble (non déjà vu) des colonnes a et b à la colonne init.

2 est final dans $\mathcal{A}_2$ non déterministe.



3. Les automates $\mathcal{A}_1$, $\mathcal{A}_2$ et les automates déterministes construits sont-ils complets ? Que remarquez-vous ?

$\mathcal{A}_1$ est complet. $\mathcal{A}_2$ n'est pas complet. $\mathcal{D}_2(\mathcal{A}_2)$ est complet.

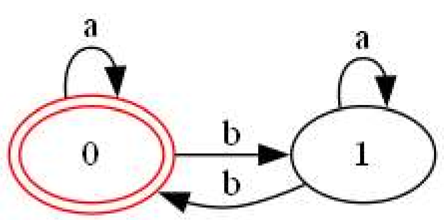
Pour compléter un automate déterminisé, on peut ajouter un état $\{\emptyset\}$ qui est un puits potentiel.

Exercice 8. Intersection et concaténation

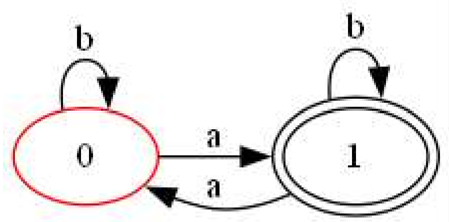
Sur $A = \{a, b\}$, soient L_1 le langage comprenant tous les mots contenant un nombre pair de b et L_2 le langage comprenant tous les mots contenant un nombre impair de a.

1. Donner pour chaque L_i un automate $\mathcal{A}_i$ reconnaissant L_i.

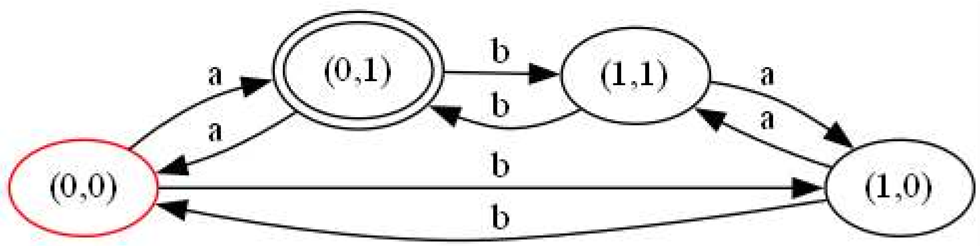
$\mathcal{A}_1$:



$\mathcal{A}_2$:



2. Calculer à partir des $\mathcal{A}_i$ un automate reconnaissant $L_1 \cap L_2$.



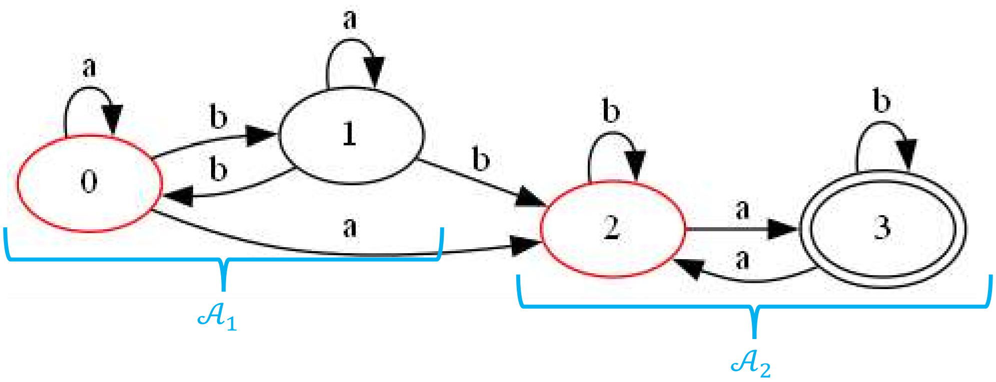
3. Construire à partir des $\mathcal{A}_i$ un automate reconnaissant $L_1.L_2$.

Rappel : construire la concaténation de deux automates

- renommer les états dans $\mathcal{A}_2$
- les états de la concaténation sont l'union des états des deux automates
- s'il n'existe pas d'état à la fois initial et final dans $\mathcal{A}_1$, les états initiaux de la concaténation sont les états initiaux de $\mathcal{A}_1$; sinon $I = I_1 \cup I_2$
- pour chaque transition de $\mathcal{A}_1$ vers un état final de $\mathcal{A}_1$, changer l'état final par chaque état initial de $\mathcal{A}_2$ (on rajoute autant de transition à la concaténation que d'état initiaux de $\mathcal{A}_2$)

Il n'y a plus d'états finaux dans $\mathcal{A}_1$.

La concaténation ne préserve pas le déterministe.



$\mathcal{A}_1$ accepte le mot vide donc 2 (0 dans $\mathcal{A}_2$) reste un état initial pour permettre à la partie du mot correspondant à $\mathcal{A}_1$ d'être vide.

On a ajouté les transitions (1, b, 2) et (0, a, 2).

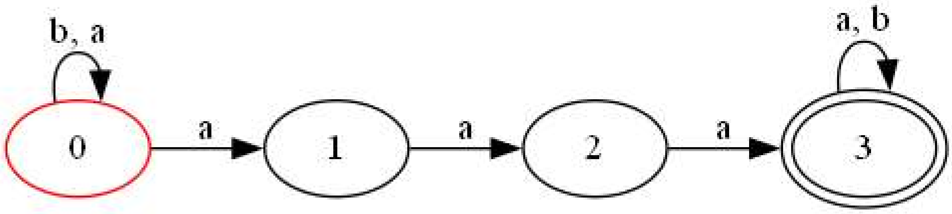
Exercice 9

Soit $A = \{a, b\}$ et soit L le langage comprenant tous les mots ayant trois occurrences successives de « a ». Donner un automate non déterministe reconnaissant L et construire un automate déterministe acceptant L.

$L = \{\text{mots avec facteur } aaa = a^3\}$

<u>automate non-déterministe</u>

$\mathcal{A}$:



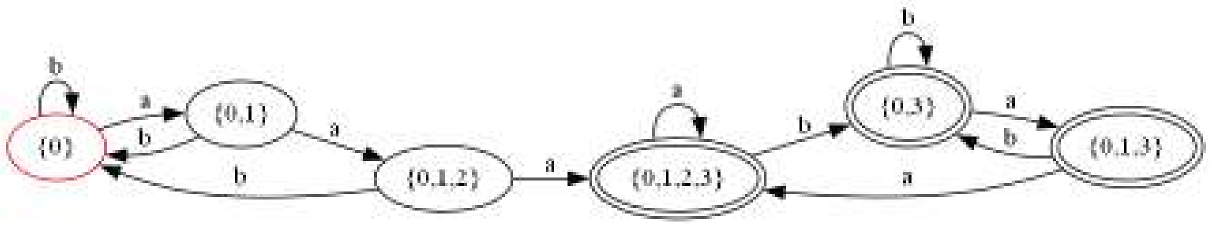
<u>automate déterministe</u>

$\mathcal{P}(\{0,1,2,3\})$

	a	b
$\{0\}$	$\{0,1\}$	$\{0\}$
$\{0,1\}$	$\{0,1,2\}$	$\{0\}$
$\{0,1,2\}$	$\{0,1,2,3\}$	$\{0\}$
$\{0,1,2,3\}$	$\{0,1,2,3\}$	$\{0,3\}$
$\{0,3\}$	$\{0,1,3\}$	$\{0,3\}$
$\{0,1,3\}$	$\{0,1,2,3\}$	$\{0,3\}$

$\{0,1,2,3\}$, $\{0,3\}$ et $\{0,1,3\}$ contiennent un état final de l'automate (3) donc c'est un état final de l'automate déterminisé.

$\mathcal{D}$:



Exercice 10. Complémentaire et différence

1. Soient L_1 et L_2 des langages sur un alphabet A. Montrer que si L_1 et L_2 sont respectivement reconnaissables par des automates $\mathcal{A}_1$ et $\mathcal{A}_2$ alors le langage $L_1 \setminus L_2$ est reconnaissable par un automate.

L_1 est reconnu par $\mathcal{A}_1$ et L_2 est reconnu par $\mathcal{A}_2$.

On cherche à construire un automate $\mathcal{A}_3$ qui reconnaît $L_1 \setminus L_2$.

1 : On vérifie si $\mathcal{A}_2$ est complet et déterministe. Dans le cas contraire, on complète et déterminise $\mathcal{A}_2$ pour obtenir $\mathcal{D}_2$ déterministe et complet.

2 : A partir de $\mathcal{D}_2$, on construit l'automate $\mathcal{A}_3$ qui reconnaît le langage L_3 complémentaire de L_2 : $L_3 = A^* \setminus L_2$. On obtient $\mathcal{A}_3$ en inversant les états finaux et non finaux.

Rappel : construire le complémentaire d'un automate

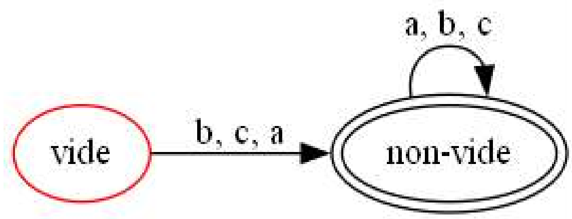
L'automate de départ doit être déterministe et complet. Si nécessaire on déterminise puis on complète l'automate, ou inversement. On construit le complémentaire en inversant ses états finaux et non finaux. Un état non final devient final et un état final devient non final.

A^* est l'ensemble de tous les mots construits avec l'alphabet A, y compris le mot vide.

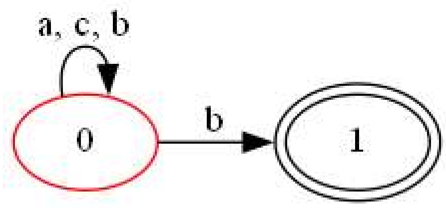
3 : On construit l'intersection $\mathcal{A}_1 \cap \mathcal{A}_3$ des automates $\mathcal{A}_1$ et $\mathcal{A}_3$, qui est l'automate qui reconnaît le langage $L_1 \setminus L_2$.

2. Construire un automate déterministe sur l'alphabet $A = \{a, b, c\}$ pour l'ensemble des mots non vides ne se terminent pas par « b ». Cette construction sera faite de deux façons.
   (a) En utilisant le résultat ci-dessus à partir d'un automate $\mathcal{A}_1$ acceptant les mots non vides et de l'automate non déterministe (qu'on appellera $\mathcal{A}_2$) de l'exercice 6 question 3.

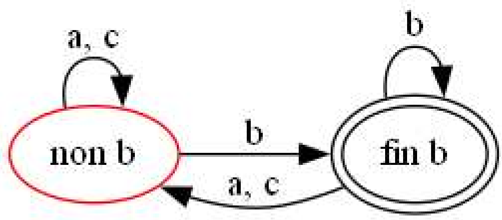
$\mathcal{A}_1$: {mots non vides}



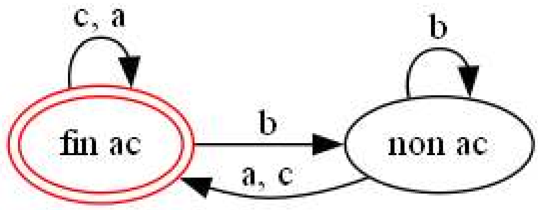
$\mathcal{A}_2$ (non-déterministe) : {mots se terminant par 'b'}



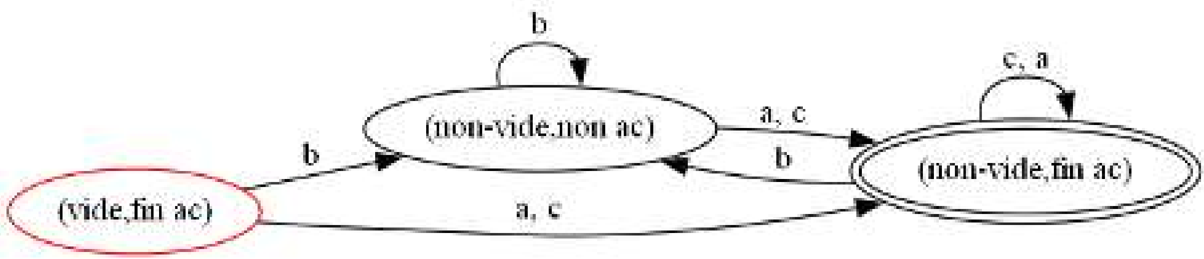
$\mathcal{D}_2$ (version déterministe de $\mathcal{A}_2$) :



$\mathcal{A}_3$ (complémentaire de $\mathcal{D}_2$) : {mots <u>ne</u> se terminant <u>pas</u> par 'b'}

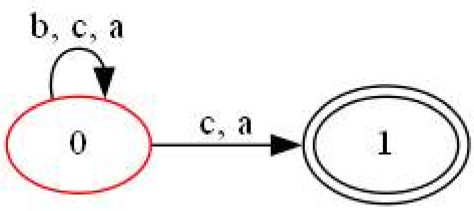


Intersection de $\mathcal{A}_1$ et $\mathcal{A}_3$:



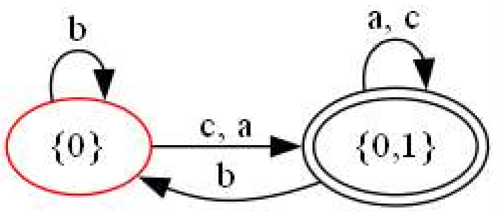
   (b) En déterminisant l'automate (qu'on appellera $\mathcal{A}_4$) de l'exercice 6 question 4.

$\mathcal{A}_4$:



	a	b	c
{0}	{0,1}	{0}	{0,1}
{0,1}	{0,1}	{0}	{0,1}

$\mathcal{D}_4$:



Les automates (a) et (b) reconnaissent le même langage et sont tous les deux complets et déterministes. La différence est que (a) a un état de plus que (b). (b) est un automate minimal (les automates minimaux ne sont plus au programme de l'UE).

5 Systèmes d'équations et expressions rationnelles

Exercice 11. Lemme d'Arden

On rappelle ici l'énoncé :

Soient K et M deux langages de A^* tels que $\varepsilon \notin K$, alors l'équation $X = K.X + M$ (qui s'écrit aussi $X = K.X \cup M$, la notation $+$ représentant l'union) admet pour unique solution le langage $K^*.M$.

Démontrez-le.

$$X = \underbrace{K}_{(\varepsilon \notin K)}.X \underbrace{+}_{\cup} M \Rightarrow X = K^*.M$$

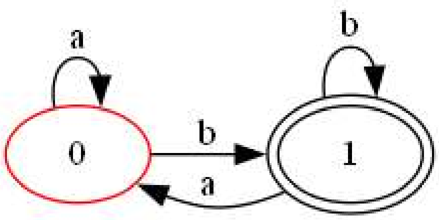
Exercice 12

Rappel : méthode pour utiliser le lemme d'Arden

- On traduit l'automate en un système d'équations, 1 équation par état. Pour trouver l'équation d'un état, on associe à chaque étiquette son état de destination et on sépare les paires étiquettes/destination par « + ».
- On part de l'état final, on applique le lemme d'Arden dessus. On remplace dans l'état au-dessus.
- On réécrit l'équation de l'état d'au-dessus de manière à appliquer le lemme d'Arden sur l'état d'au-dessus. On remplace dans l'état d'au-dessus.
- On applique le lemme d'Arden sur l'état d'au-dessus…

1. Soit l'automate $\mathcal{A}$ d'états 0, 1, d'état initial 0, d'état terminal 1 et de transitions (0, a, 0), (0, b, 1), (1, a, 0) et (1, b, 1). Dessiner l'automate $\mathcal{A}$. Soit L le langage reconnu par $\mathcal{A}$. Donner le système d'équations associé à $\mathcal{A}$ et en déduire une expression rationnelle pour L.

$\mathcal{A}$:



(L_0) (L_1)

Système d'équations :

(1) $L_0 = \underbrace{a}_{K} L_0 + \underbrace{bL_1}_{M}$

(2) $L_1 = \underbrace{aL_0}_{M} + \underbrace{b}_{K} L_1 \underbrace{+\varepsilon}_{M}$

Si un état est final, on accepte aussi le mot vide.

L_0 est le langage accepté par l'état 0. L_1 est le langage accepté par l'état 1.

On applique Arden sur (2) :

$$L_1 = \underbrace{b}_{K} L_1 + \underbrace{(aL_0 + \varepsilon)}_{M} \Rightarrow L_1 = b^*(aL_0 + \varepsilon)$$

$$L_1 = b^* a L_0 + b^*$$

On remplace la solution de L_1 dans (1) :

$L_0 = aL_0 + b(b^*aL_0 + b^*)$

$L_0 = aL_0 + bb^*aL_0 + bb^*$

$L_0 = \underbrace{(a + bb^*a)}_{K} L_0 + \underbrace{bb^*}_{M}$

On applique Arden :

$L_0 = (a + bb^*a)^*.bb^*$

On factorise par a.

$L_0 = \left((\varepsilon + bb^*)a\right)^* bb^*$

$L_0 = (b^*a)^*bb^*$

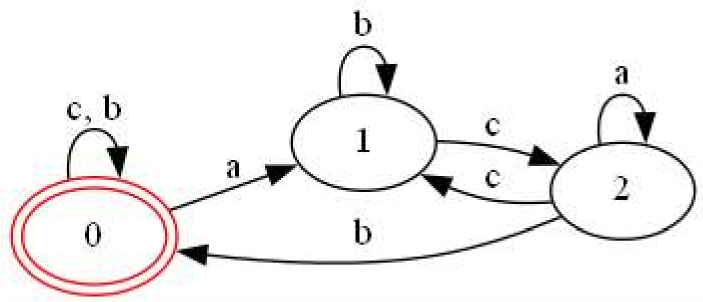
ε est neutre par concaténation $\Rightarrow$ $(\varepsilon + bb^*)a$ devient b^*a car

- soit on lit un a sans b du tout
- soit on lit un b (éventuellement des autres b) et un a

Si on écrit bb^*a, on impose au moins un b donc perd la possibilité de commencer par a.

2. Mêmes questions avec $\mathcal{B}$ d'états 0, 1, 2, d'état initial 0, d'état terminal 0 et de transitions (0, a, 1), (0, b, 0), (0, c, 0), (1, b, 1), (1, c, 2), (2, a, 2), (2, b, 0) et (2, c, 1).

$\mathcal{B}$:



Système : $\begin{cases} L_0 = aL_1 + bL_0 + cL_0 + \varepsilon \quad (\text{car } 0 \text{ final}) \\ L_1 = bL_1 + cL_2 \\ L_2 = aL_2 + bL_0 + cL_1 \end{cases} \Leftrightarrow \begin{cases} L_0 = aL_1 + (b+c)L_0 + \varepsilon \\ L_1 = bL_1 + cL_2 \\ L_2 = aL_2 + bL_0 + cL_1 \end{cases}$

On applique Arden sur la 3e équation :

$L_2 = \underbrace{a}_{K} L_2 + \underbrace{bL_0 + cL_1}_{M} \Rightarrow L_2 = a^*(bL_0 + cL_1)$

On remplace L_2 par la solution dans la 2e équation :

$L_1 = bL_1 + cL_2 \Rightarrow L_1 = bL_1 + ca^*(bL_0 + cL_1)$

On simplifie L_1 :

$L_1 = bL_1 + ca^*bL_0 + ca^*cL_1$

$L_1 = \underbrace{(b + ca^*c)}_{K} L_1 + \underbrace{ca^*bL_0}_{M}$ (factorisation par L_1)

On applique Arden sur la 2e équation :

$L_1 = (b + ca^*c)^*.ca^*bL_0$

6 Langages reconnaissables

Rappel : langage reconnaissable

Un langage est reconnaissable si et seulement si il peut être reconnu par un automate fini.
Un langage qui peut s'écrire avec des a^*, b^* et des concaténations est reconnaissable.
$A = \{a, b\}$
$a^*.b^*$ reconnaissable

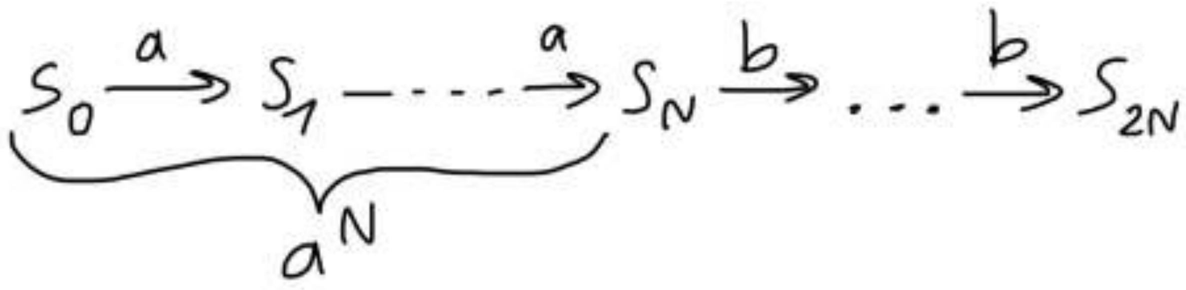
Exercice 16

Montrer que le langage $L = \{a^n b^n, n \geq 0\}$ sur l'alphabet $\{a, b\}$ ne peut pas être reconnu par un automate fini.

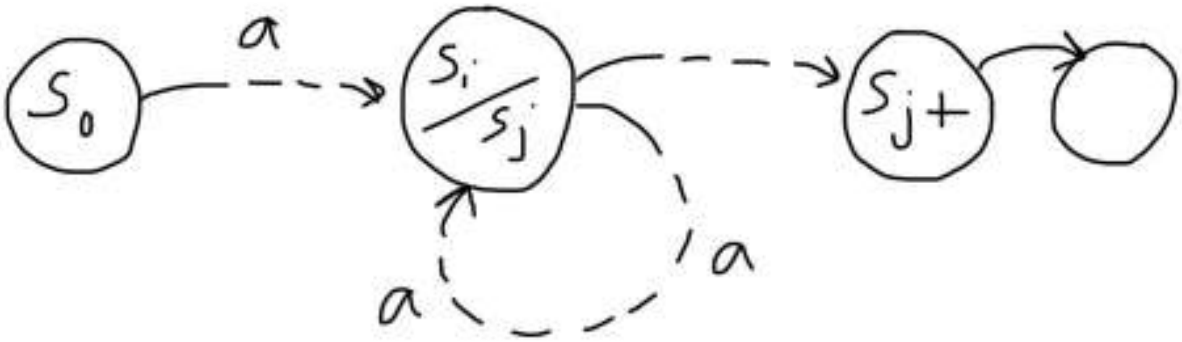
Brouillon

$aabb \in L$ $abb \notin L$
Si $\mathcal{A}$ reconnaît $L \rightarrow$ il existe un chemin d'un état initial à terminal étiqueté par $a^n b^n$, n fixé
Le nombre d'état de l'automate est fini, mais $n \rightarrow \infty$, donc on boucle à un moment.

Par l'absurde, on suppose qu'il existe un automate $\mathcal{A}$ qui reconnaît L.
Comme le nombre d'états de $\mathcal{A}$ est fini, on peut considérer N strictement plus grand que le nombre d'états de A soit alors



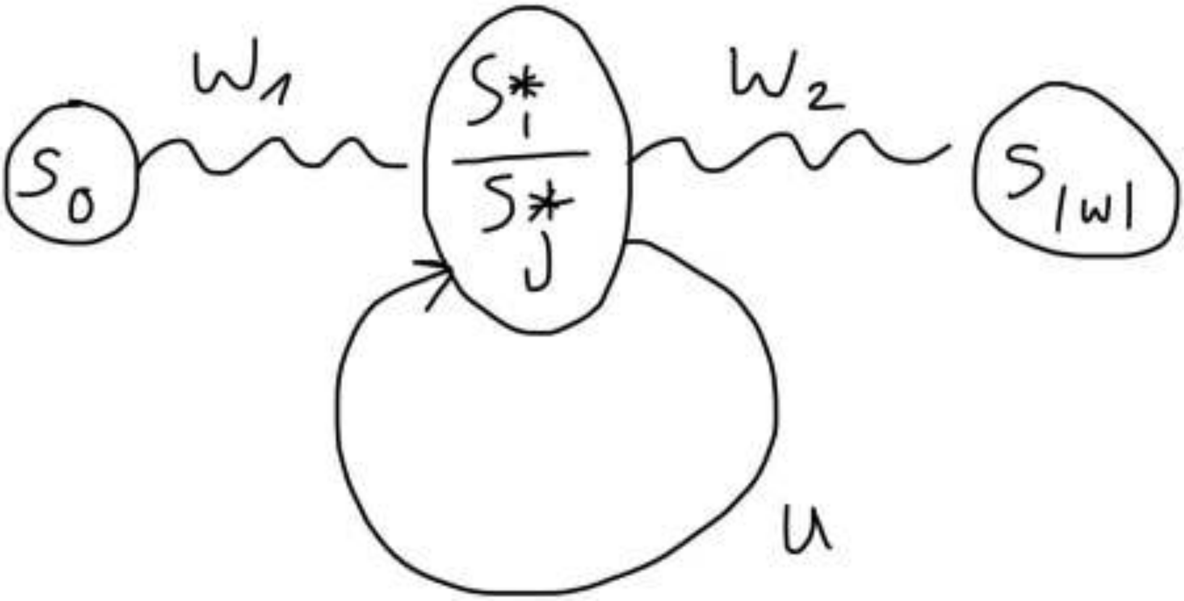
Comme $N >$ le nombre d'états, il existe $(i, j) \in \{0, \cdots, N\}^2$, $i \neq j$ tels que $q = s_i = s_j$. Ainsi, le mot $u = a^i . a^{N-j} . b^N$ est reconnu par $\mathcal{A}$ avec $i \neq j$, ce qui est impossible.



Exercice 17. Lemme de l'étoile

Soit L un langage reconnaissable par un automate fini. Montrer qu'il existe un entier N_0 tel que pour tout mot $w \in L$ vérifiant $|w| \geq N_0$ (où $|w|$ est la longueur de w), on a $w = w_1 u w_2$ avec

1. $u \neq \varepsilon$,
2. $|u| < N_0$,
3. $w_1 u^* w_2 \subseteq L$



Soit L un langage reconnaissable et $\mathcal{A}$ un automate (fini) qui reconnaît L.

Soit N_0 un entier strictement supérieur au nombre d'états de $\mathcal{A}$.

Soit $w \in L$ de longueur $|w| \geq N_0$.

Soit la suite d'états $s_0 \cdots s_{|w|}$ le chemin de $\mathcal{A}$ associé à w.

Comme $|w| \geq N_0$, il existe au moins un couple $(i, j) \in \{0, \cdots, |w|\}^2$ avec $i \neq j$ et $q = s_i = s_j$.

Soit (i^*, j^*) tel que $j^* - i^*$ soit minimum.

Soit $w = w_1 u w_2$.

- w_1 correspond au chemin de s_0 à s_{i^*}
- u correspond au chemin de s_{i^*} à s_{j^*}
- w_2 corrrespond au chemin de s_{j^*} à $s_{|w|}$

1) $i^* \neq j^*$ donc $u \neq \varepsilon$
2) $|u| < N_0$
   Par l'absurde, si $|u| \geq N_0$, alors il y a un autre couple $(i, j) \in \{0, \cdots, |w|\}^2$ avec $q' = s_i = s_j$ et $i^* \leq i$ et $j \leq j^*$. Dans ce cas, $j - i < j^* - i^*$. Ce qui est absurde avec l'hypothèse $j^* - i^*$ minimum.
3) Tout élément de $w_1 u^* w_2$ correspond bien à un chemin d'un état initial à final dans $\mathcal{A}$. Donc, $w_1 u^* w_2 \subseteq L$.

Exercice 18

Montrer, en utilisant le lemme de l'étoile, que les langages suivants sur l'alphabet $\{a, b\}$ ne peuvent pas être reconnus par un automate fini.

2. $L_2 = \{a^p, p \text{ premier}\}$.

Pour démontrer qu'un langage ne peut pas être reconnu par un automate fini, on utilise le lemme de l'étoile avec un raisonnement par l'absurde.

Par l'absurde, on suppose que L_2 est reconnaissable.

D'après le lemme de l'étoile, il existe N_0 tel que pour $p \geq N_0$, p premier vérifie les 3 propriétés du lemme.

$w = a^p = a^\alpha . a^\beta . a^\gamma$ avec $\alpha + \beta + \gamma = p$.

D'après la propriété 3, $a^{\alpha+\beta+\gamma} \in L_2, \forall k \in \mathbb{N}$.

D'après la propriété 2, $\beta < N_0$ donc $\alpha + \gamma > 0$.

Tous les nombres sont entiers.
(1) $\alpha + \beta + \gamma = p$
(2) $\beta < N_0 \Rightarrow \beta \leq N_0 - 1$
(3) $p \geq N_0 + 1$
(1) $\alpha + \gamma = p - \beta \geq N_0 + 1 - (N_0 + 1)$
$\alpha + \gamma \geq 2$

Si on pose $k = \alpha + \gamma$.

$$\begin{aligned}\alpha + k\beta + \gamma &= \alpha + (\alpha + \gamma)\beta + \gamma \\ &= (\beta + 1)(\alpha + \gamma)\end{aligned}$$

$\beta + 1 \geq 2$ car $u \neq \varepsilon$

$\alpha + \gamma \geq 2$

donc $\alpha + k\beta + \gamma$ n'est pas premier, il n'appartient donc pas à L_2, ce qui est contraire au lemme de l'étoile.

Exercice 19

Les langages ci-dessous sont-ils reconnaissables ?

1. $L = \{a^n b^n \mid n, p \geq 0, n = p \bmod 3\}$

Oui, il faut construire l'automate qui reconnaît L pour le prouver.

2. $L' = \{a^m b^n \mid m \geq 1, n \geq 1, m \neq n\}$

Non, il faut se servir du complémentaire (et de la différence de deux langages) pour le prouver.

TD 6 : Logique

Exercice 1. Fonctions booléennes

Rappels

En français : a ou b

En mathématiques :

$a + b$ OU inclusif

XOR(a, b) OU exclusif

Forme normal disjonctive : on exprime les 1 de la table de vérité, séparés par $+$

Forme normal conjonctive : on exprime les 0 de la table de vérité, séparés par $\cdot$

Les formes normales disjonctive et conjonctive ne sont pas uniques.

1. Construire la table de vérité de la fonction booléenne correspondant à l'opérateur booléen « ou exclusif », noté *XOR*, et donner une expression booléenne associée. Donner des formes normales disjonctives et conjonctives de cette fonction.

a	b	*XOR*
0	0	0
0	1	1
1	0	1
1	1	0

FND : $XOR(a, b) = \bar{a}b + a\bar{b}$

FNC : $XOR(a, b) = (a + b)(\bar{a} + \bar{b})$

2. Donner une expression booléenne pour la fonction f définie par :

x	y	$f(x, y)$
0	0	1
0	1	0
1	0	0
1	1	0

et en donner une forme normale conjonctive.

FND : $f(x, y) = \bar{x}\bar{y}$

FNC : $f(x, y) = (x + \bar{y})(\bar{x} + y)(\bar{x} + \bar{y})$

3. Donner une expression booléenne pour la fonction g définie par :

x_1	x_2	x_3	$g(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	1
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	0

Tableau de Karnaugh :

x_1x_2 \ x_3	0	1
00	0	1
01	1	1
11	0	0
10	0	1

$$g(x_1, x_2, x_3) = \overline{x_1}x_2 + \overline{x_2}x_3$$

Méthode : trouver la forme normale conjonctive à partir de la forme normale disjonctive

Lorsqu'on a l'expression sous forme normale disjonctive, on fait 2 fois le complémentaire (complémentaire une première fois, développer et réduire, puis faire le complémentaire une deuxième fois).

$$\bar{g} = \overline{\overline{x_1}x_2 + \overline{x_2}x_3}$$
$$\bar{g} = \overline{\overline{x_1}x_2} \cdot \overline{\overline{x_2}x_3}$$
$$\bar{g} = (x_1\overline{x_2})(x_2\overline{x_3})$$
$$\bar{g} = x_1x_2 + x_1\overline{x_3} + \underbrace{\overline{x_2}x_2}_{0} + \overline{x_2}\,\overline{x_3}$$
$$g = \overline{x_1x_2 + x_1\overline{x_3} + \overline{x_2}\,\overline{x_3}}$$
$$g = (\overline{x_2}\,\overline{x_2})(\overline{x_1}x_3)(x_2x_3)$$

4. Donner une forme normale conjonctive pour la fonction $h(x,y,z) = xy + yz + xz$.

$h = xy + yz + xz$

$\bar{h} = \overline{xy + yz + xz}$

$\bar{h} = (\bar{x} + \bar{y}) \cdot (\bar{y} + \bar{z})(\bar{x} + \bar{z})$

$\bar{h} = (\bar{x}\bar{y} + \bar{x}\bar{z} + \bar{y} + \bar{y}\bar{z})(\bar{x} + \bar{z})$

On factorise par $\bar{y}$:

$\bar{x}\bar{y} + \bar{y} + \bar{y}\bar{z} = \bar{y}(\bar{x} + 1 + \bar{z}) = \bar{y} \cdot 1 = \bar{y}$

$\bar{h} = (\bar{y} + \bar{x}\bar{z})(\bar{x} + \bar{z})$

$\bar{x}\bar{z}\bar{x} \to \bar{x}\bar{x} = \bar{x}$

$\bar{h} = \bar{y}\bar{x} + \bar{y}\bar{z} + \bar{x}\bar{z}$

$h = \overline{\bar{y}\bar{x} + \bar{y}\bar{z} + \bar{x}\bar{z}}$

$h = \overline{\bar{y}\bar{x}} \cdot \overline{\bar{y}\bar{z}} \cdot \overline{\bar{x}\bar{z}}$

$h = (x + y)(y + z)(x + z)$ FNC

Exercice 2. Formules logiques et fonction booléennes

On considère la formule F suivante : $(p \wedge q \wedge \neg r) \vee (p \wedge \neg q \wedge r) \vee (\neg p \wedge q \wedge r)$

1. Les formules F et $\neg F$ sont-elles satisfiables ? Sont-elles valides (des tautologies) ? Donner des formes normales conjonctives et disjonctives pour les fonctions booléennes représentant ces formules.

Rappel : formules satisfiables et valides

formule satisfiable : $\exists \mathrm{I}, \mathrm{I}(F) = 1$
formule valide : $\forall \mathrm{I}, \mathrm{I}(F) = 1$

$\mathrm{I}(p) = 1$	$\mathrm{I}(p) = 1$
$\mathrm{I}(q) = 1$	$\mathrm{I}(q) = 1$
$\mathrm{I}(r) = 0$	$\mathrm{I}(r) = 1$
$\mathrm{I}(F) = 1 \cdot 1 \cdot 1 = 1$	$\mathrm{I}(F) = 1 \cdot 1 \cdot 0 + 1 \cdot 0 \cdot 1 + 0 \cdot 1 \cdot 1 = 0$
F est satisfiable.	$\neg F$ est satisfiable.

F n'est pas valide, car $\neg F$ est satisfiable.

$\neg F$ n'est pas valide car F est satisifiable.

$f(x,y,z) = xy\bar{z} + x\bar{y}z + \bar{x}yz$ FND de f

$\bar{f}(x,y,z) = \overline{xy\bar{z} + x\bar{y}z + \bar{x}yz}$

$\bar{f}(x,y,z) = \overline{xy\bar{z}} \cdot \overline{x\bar{y}z} \cdot \overline{\bar{x}yz}$

$\bar{f}(x,y,z) = (\bar{x} + \bar{y} + z)(\bar{x} + y + \bar{z})(x + \bar{y} + \bar{z})$ FNC de $\bar{f}$

$\bar{f}(x,y,z) = (\bar{x}\bar{x} + \bar{x}y + \bar{x}\bar{z} + \bar{y}\bar{x} + \bar{y}y + \bar{y}\bar{z} + z\bar{x} + zy + z\bar{z})(x + \bar{y} + \bar{z})$

$\bar{x}\bar{x} = \bar{x}$ et $\bar{y}y = 0$ et $z\bar{z} = 0$ donc

$\bar{f}(x,y,z) = (\bar{x} + \bar{x}y + \bar{x}\bar{z} + \bar{y}\bar{x} + \bar{y}\bar{z} + z\bar{x} + zy)(x + \bar{y} + \bar{z})$

On peut simplifier par $\bar{x}$:

$\bar{f}(x,y,z) = (\bar{x} + \bar{y}\bar{z} + zy)(x + \bar{y} + \bar{z})$

$\bar{f}(x,y,z) = \bar{x}x + \bar{x}\bar{y} + \bar{x}\bar{z} + \bar{y}\bar{z}x + \bar{y}\bar{z}\bar{y} + \bar{y}\bar{z}\bar{z} + zyx + zy\bar{y} + zy\bar{z}$

$\bar{f}(x,y,z) = \bar{x}\bar{y} + \bar{x}\bar{z} + \bar{y}\bar{z}x + \bar{y}\bar{z} + \bar{y}\bar{z} + zyx$

On peut simplifier par $\bar{y}\bar{z}$:

$\bar{f}(x,y,z) = \bar{x}\bar{y} + \bar{x}\bar{z} + \bar{y}\bar{z} + zyx$ FND de $\bar{f}$

$f(x,y,z) = \overline{\bar{x}\bar{y} + \bar{x}\bar{z} + \bar{y}\bar{z} + zyx}$

$f(x,y,z) = (x + y)(x + z)(y + z)(\bar{z} + \bar{y} + \bar{x})$ FNC de f

2. Déterminer une formule G telle que $(F \wedge G) \vee (\neg F \wedge \neg G)$ soit une formule valide (i.e. une tautologie).

$G = F$

$(F \wedge F) \vee (\neg F \wedge \neg F) = F \vee \neg F$ Toujours vraie/Valide

Exercice 3. Enigme

Anna et Mathias sont accusés d'un crime. Il font les déclarations suivantes :

Anna : Mathis est coupable.

Mathias : Nous sommes tous les deux innocents.

1. On suppose que tous les deux ont menti. Peut-on déterminer qui est coupable, qui ne l'est pas ?

p : Mathias est innocent

q : Anna est innocente

Anna : $\neg p$

Mathias : $p \wedge q$

On suppose que p est vraie et $\neg(p \wedge q)$ est vraie.

$\neg(p \wedge q) = \neg p \wedge \neg q$

Si p est vraie, alors $\neg p$ est faux. Pour que $\neg p \wedge \neg q$ soit vraie, $\neg q$ doit être vraie.

On a donc forcément $\neg q$. Mathias est innocent, Anna est coupable.

2. On suppose maintenant que les coupables mentent et que les innocents disent la vérité. Peut-on déterminer qui est coupable, qui ne l'est pas ?

$$\begin{cases} q \to \neg p \\ \neg q \to p \\ p \to p \wedge q \\ \neg p \to \neg(p \wedge q) \end{cases}$$

Soit I une interprétation telle que

$$\begin{cases} \mathrm{I}(q \to \neg p) = 1 \\ \mathrm{I}(\neg q \to p) = 1 \\ \mathrm{I}(p \to p \wedge q) = 1 \\ \mathrm{I}\big(\neg p \to \neg(p \wedge q)\big) = 1 \end{cases}$$

$\overline{\mathrm{I}(q)} + \overline{\mathrm{I}(p)} = 1$

$\mathrm{I}(q) + \mathrm{I}(p) = 1$

$\overline{\mathrm{I}(p)} + \mathrm{I}(p)\mathrm{I}(q) = 1$

$\mathrm{I}(p) + \overline{\mathrm{I}(p)\mathrm{I}(q)} = 1$

$\mathrm{I}(q) = 1$ et $\mathrm{I}(p) = 0$ est une solution.

$\mathrm{I}(q) = 0$ et $\mathrm{I}(p) = 1$ ne marche pas.

L'unique solution est $\mathrm{I}(q) = 1$ et $\mathrm{I}(p) = 0$.

Anna est innocente, Mathias est coupable.

Exercice 4. Conséquence sémantique

Les conséquences sémantiques suivantes sont-elles vérifiées ?

$F1 \vDash F2 \Leftrightarrow F1$ est la conséquence logique de $F2$.

1. $p \to q \vDash \neg q \to \neg p$

C'est la contraposée.

Soit I une interprétation telle que $\mathrm{I}(p \to q) = 1$.

$\overline{\mathrm{I}(q)} + \mathrm{I}(q) = 1$

$\mathrm{I}(\neg q \to \neg p) = \overline{\mathrm{I}(\neg q)} + \mathrm{I}(\neg p) = \mathrm{I}(q) + \overline{\mathrm{I}(p)} = 1$

Donc le séquent ($\vDash$) est vérifié.

2. $p \to q \vDash q \neg p$

Soit $\mathrm{I}(p) = 0$ et $\mathrm{I}(q) = 1$.

$\mathrm{I}(p \to q) = \overline{\mathrm{I}(p)} + \mathrm{I}(q) = 1$

$\mathrm{I}(q \to p) = \overline{\mathrm{I}(q)} + \mathrm{I}(p) = 0$

Donc le séquent n'est pas vérifié.

5. $\{p \vee q, p \to r, q \to r\} \vDash r$

Soit I une interprétation telle que $\mathrm{I}(p \vee q) = 1$, $\mathrm{I}(p \to r) = 1$ et $\mathrm{I}(q \to r) = 1$.

On résout le système :

$$\begin{cases} \mathrm{I}(p) + \mathrm{I}(q) = 1 \\ \overline{\mathrm{I}(p)} + \mathrm{I}(r) = 1 \\ \overline{\mathrm{I}(q)} + \mathrm{I}(r) = 1 \end{cases}$$

Si $\mathrm{I}(p) = 1$, alors $\mathrm{I}(r) = 1$ ($\mathrm{I}(q) \in \{0,1\}$).

Si $\mathrm{I}(p) = 0$, alors $\mathrm{I}(q) = 1$ et $\mathrm{I}(r)1$.

Dans tous les cas $\mathrm{I}(r) = 1$. Donc le séquent est valide.

Exercice 6. Formules valides, formules satisfiables

Les formules suivantes sont-elles satisfiables ? sont-elles valides (des tautologies) ?

(2) $\big((p \vee q) \wedge \neg p\big) \rightarrow p$

satisfiable	**validité**
Si $\mathrm{I}(q) = 1$ et $\mathrm{I}(p) = 0$.	$\mathrm{I}(p) = 1$ et $\mathrm{I}(q) = 1$
$\mathrm{I}\big((p \vee q) \wedge \neg p\big) = \big(\mathrm{I}(p) + \mathrm{I}(q)\big) \cdot \overline{\mathrm{I}(p)} = 1$	$\mathrm{I}\big((p \vee q) \wedge \neg p\big) = \big(\mathrm{I}(p) + \mathrm{I}(q)\big) \cdot \overline{\mathrm{I}(p)} = 0$
(2) est satisfiable.	(2) n'est pas valide.
On aurait pu prendre $\mathrm{I}(q) = 0$.	

Exercice 9. Enigme

C'est un type d'exercice susceptible de tomber à l'examen.

1. Soit f la fonction booléenne à 3 variables définie par :
   $f(x, y, z) = (\bar{x}z + \bar{y})(\bar{x} + \bar{y}\bar{z})(xy + yz + xz)$
   (a) La fonction f est-elle sous forme normale conjonctive ? disjonctive ?

ni une FNC

ni une FND

   (b) Donner une forme normale disjonctive pour f et en déduire une forme normale conjonctive.

$f(x, y, z) = (\bar{x}z + \bar{y})(\bar{x} + \bar{y}\bar{z})(xy + yz + xz)$

$f(x, y, z) = (\bar{x}z + \bar{y}\bar{x} + \bar{y}\bar{z})(xy + yz + xz)$

$f(x, y, z) = \bar{x}yz$ FNC et FND

2. Le lendemain de Noël, on retrouve une boîte de chocolats totalement vide. Pour trouver les coupables qui ont mangé des chocolats, on interroge les trois enfants qui font les déclarations suivantes :
   Anissa : (A) Si Boris est coupable alors Charlotte aussi et je suis innocente.
   Boris : (B) Au moins deux d'entre nous ont mangé des chocolats.
   Charlotte : (C) Si Anissa est coupable alors Boris et moi sommes innocents.
   (a) Exprimer chacune des trois déclarations A, B et C comme une formule, à l'aide des propositions p : *Anissa a mangé des chocolats*, q : *Boris a mangé des chocolats*, r : *Charlotte a mangé des chocolats*.

A : $q \rightarrow r \wedge \neg p$

B : $(p \wedge q) \vee (q \wedge r) \vee (p \wedge r)$

C : $p \rightarrow \neg q \wedge \neg r$

(b) Pour une interprétation I, calculer les interprétations de ces trois formules $\mathrm{I}(A)$, $\mathrm{I}(B)$ et $\mathrm{I}(C)$, en fonction de $\mathrm{I}(p)$, $\mathrm{I}(q)$ et $\mathrm{I}(r)$.

$\mathrm{I}(A) = \overline{\mathrm{I}(q)} + \mathrm{I}(r) \cdot \overline{\mathrm{I}(q)}$ $\quad \rightarrow \bar{x}z + \bar{y}$

$\mathrm{I}(B) = \mathrm{I}(p)\mathrm{I}(q) + \mathrm{I}(q)\mathrm{I}(r) + \mathrm{I}(p)\mathrm{I}(r)$ $\quad \rightarrow xy + yz + xz$

$\mathrm{I}(C) = \overline{\mathrm{I}(p)} + \overline{\mathrm{I}(q)} \cdot \overline{\mathrm{I}(r)}$ $\quad \rightarrow \bar{x} + \bar{y}\bar{z}$

$x \leftrightarrow \mathrm{I}(p) \qquad y \leftrightarrow \mathrm{I}(q) \qquad z \leftrightarrow \mathrm{I}(r)$

(c) On suppose que les trois enfants disent la vérité. Que peut-on déduire sur la réponse à la question : qui a mangé des chocolats ?

les trois enfants disent la vérité $\Leftrightarrow \mathrm{I}(A) \cdot \mathrm{I}(B) \cdot \mathrm{I}(C) = 1$

$\mathrm{I}(A) \cdot \mathrm{I}(B) \cdot \mathrm{I}(C) = \overline{\mathrm{I}(p)} \cdot \mathrm{I}(q) \cdot \mathrm{I}(r) = 1$

Les trois termes doivent être à 1.

$\mathrm{I}(p) = 0$, $\mathrm{I}(q) = 1$ et $\mathrm{I}(r) = 1$

Boris et Charlotte ont mangé des chocolats.

(d) Après une enquête plus approfondie, il s'avère que Boris et Anissa sont coupables et Charlotte innocente. En utilisant (b), dire qui a menti et qui a dit la vérité.

$$\begin{cases} \mathrm{I}(q) = 1 \\ \mathrm{I}(p) = 1 \\ \mathrm{I}(r) = 0 \end{cases} \Rightarrow \begin{cases} \mathrm{I}(A) = 0 \\ \mathrm{I}(B) = 1 \\ \mathrm{I}(C) = 0 \end{cases}$$

Anissa et Charlotte ont menti, Boris dit la vérité.