LOG 2810: Structures discrètes

Partie 1 : Introduction au raisonnement mathématique.

Julien Dompierre, Philippe Galinier, Robert Roy

Mis à jour par

John Mullins, Fayçal Abouzaid et Foutse Khomh

Ecole Polytechnique de Montréal

Liste des Chapitres

Notions Préliminaires de Logique

logique propositionnelle - Logique du premier ordre.

Motivations

- Les mathématiques discrètes sont le fondement de l’informatique,
  - Structures de données, étude des algorithmes,
  - Étude des bases de données, automatisation,
  - Compilation, systèmes d’exploitation, sécurité, ...
- Fournir les bases mathématiques pouvant servir de passerelles vers des cours plus avancés,
- Cerner des problèmes susceptibles d’être résolus par des algorithmes,
- Décrire les procédés mis en oeuvre dans la résolution de ces problèmes, (pseudo-code et code)

Définition: énoncé

Un **énoncé** est une déclaration, i.e., une phrase qui exprime une pensée complète, un état de fait.

Exemples d'énoncés:

- Le Canadien de Montréal n'a pas gagné la coupe Stanley l'année dernière.
- $x + 1 = 3$.

Exemple de phrases qui ne sont pas des énoncés:

- Quelle heure est-il?
- Lisez ceci attentivement.

Définition: proposition

Une **proposition** est un énoncé qui peut être **vrai** ou **faux**, mais non les deux à la fois.

Exemples d'énoncés qui ne sont pas des propositions:

- Le Canadien de Montréal gagnera la coupe Stanley cette année.
- $x + 1 = 3$.

Exemple d'énoncés qui sont des propositions.

- Québec est la capitale du Canada.
- $2 + 3 = 5$.

Notation

Les lettres servent à désigner des propositions de la même façon qu'elles servent à désigner des variables. On utilise habituellement les lettres p, q, r, s, ...

La **valeur de vérité** d'une proposition est "vrai" (notée V) si cette proposition est vérifiée; la valeur de vérité est "faux" (notée F) dans le cas contraire.

Définition: proposition composée

Bien des énoncés mathématiques sont construits en combinant plusieurs propositions. Ces combinaisons forment ce qu'on appelle des **propositions composées**, lesquelles sont reliées par des opérateurs logiques (et, ou, ...).

Définition: négation

Soit p, une proposition. L'énoncé

"Il n'est pas vrai que p."

est une autre proposition, appelée **négation** de p, qui est notée $\neg p$. La proposition $\neg p$ se lit "non p".

Table de vérité de la négation

Une table de vérité présente les relations entre les valeurs de vérité de plusieurs propositions. Ces tables sont très utiles dans le cas de propositions construites à partir de propositions plus simples.

Table de vérité de la négation:

p	$\neg p$
V	F
F	V

Définition: conjonction

Soit p et q deux propositions. La proposition

"p et q",

notée $p \wedge q$, est vraie si à la fois p et q sont vraies. Elle est fausse dans tous les autres cas. Cette proposition est appelée **conjonction** de p et de q. La table de vérité de la conjonction est:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Définition: disjonction

Soit p et q deux propositions. La proposition

"p ou q",

notée $p \vee q$, est fausse si p et q sont fausses. Elle est vraie dans tous les autres cas. Cette proposition est appelée **disjonction** de p et de q. La table de vérité de la disjonction est:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

Définition: disjonction exclusive

Soit p et q deux propositions. La proposition

"p ou exclusif q",

notée $p \oplus q$, est vraie si soit p, soit q est vraie. Elle est fausse dans tous les autres cas. Cette proposition est appelée **disjonction exclusive** de p et de q. La table de vérité de la disjonction exclusive est:

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

Définition: implication

Soit p et q deux propositions. L'**implication** $p \to q$ est une proposition qui est fausse quand p est vraie et q est fausse, et qui est vraie dans tous les autres cas.

Dans cette implication, p est appelée l'**hypothèse** (ou l'**antécédent** ou la **prémisse**) et q, la **conclusion** (ou la **conséquence**).

Table de vérité de l'implication

Table de vérité de l'implication de deux propositions p et q:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

À noter:

- L'implication $p \rightarrow q$ est fausse seulement dans le cas où p est vraie et q est fausse.
- L'implication $p \rightarrow q$ est vraie si p est fausse, que q soit vraie ou fausse.

L'implication

Il existe plusieurs façons d'exprimer $p \rightarrow q$.

- "si p alors q";
- "p implique q";
- "p seulement si q";
- "p est suffisant pour que s'applique q";
- "q si p";
- "q dès que p";
- "q est nécessaire pour que p";

L'implication

Dans le langage courant, il y a une relation de cause à effet entre l'hypothèse et la conclusion d'une implication. Le concept mathématique d'implication est plus général que le sens courant. L'implication

"Si nous sommes vendredi, alors $2+3=6$."

est vraie tous les jours excepté vendredi, même si $2+3=6$ est faux. Le concept mathématique d'implication ne dépend pas d'une relation de cause à effet entre l'hypothèse et la conclusion.

Définitions: réciproque et la contraposée

Il existe certaines implications relatives à la proposition $p \to q$.

- La proposition $q \to p$ est la **réciproque** de $p \to q$.
- La proposition $\neg q \to \neg p$ est la **contraposée** de $p \to q$.

Définition: biconditionnelle

Soit p et q, deux propositions. La **biconditionnelle** $p \leftrightarrow q$ est une proposition qui est vraie quand p et q ont les mêmes valeurs de vérité et qui est fausse dans les autres cas.

Notons que la biconditionnelle $p \leftrightarrow q$ n'est vraie que si $p \rightarrow q$ et $q \rightarrow p$ sont vraies. On exprime $p \leftrightarrow q$ comme

- "p si et seulement si q";
- "p est nécessaire et suffisante pour q";
- "si p alors q et réciproquement".

Table de vérité de la biconditionnelle

Table de vérité de la biconditionnelle de deux propositions p et q:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Définitions: tautologie, contra-diction et contingence

Une proposition composée qui est toujours vraie, quelles que soient les valeurs de vérité des propositions qui la composent, est appelée une **tautologie**.

Une proposition composée qui est toujours fausse est appelée une **contradiction**.

Finalement, une proposition qui n'est ni une tautologie ni une contradiction est appelée une **contingence**.

Exemple d'une **tautologie**

La proposition composée $p \vee \neg p$ est une tautologie car elle est toujours vraie.

p	$\neg p$	$p \vee \neg p$
V	F	V
F	V	V

Exemple d'une contradiction

La proposition composée $p \wedge \neg p$ est une contradiction car elle est toujours fausse.

p	$\neg p$	$p \wedge \neg p$
V	F	F
F	V	F

Définition: équivalence logique

Les propositions p et q sont **logiquement équivalentes** si $p \leftrightarrow q$ est une tautologie. La notation $p \Leftrightarrow q$ signifie que p et q sont logiquement équivalentes.

Exemple d'équivalence logique

La table d'équivalence suivante montre que la biconditionnelle $(\neg p \vee q) \leftrightarrow (p \rightarrow q)$ est toujours vraie quelles que soient les valeurs de vérité des propositions p et q qui la composent.

p	q	$\neg p$	$\neg p \vee q$	$p \rightarrow q$	$(\neg p \vee q) \leftrightarrow (p \rightarrow q)$
V	V	F	V	V	V
V	F	F	F	F	V
F	V	V	V	V	V
F	F	V	V	V	V

Et donc $(\neg p \vee q) \Leftrightarrow (p \rightarrow q)$.

Définition: variable et prédicat

Soit l'énoncé

"x est plus grand que 3".

- Cet énoncé n'est pas une proposition car on ne peut pas se prononcer sur sa valeur de vérité.
- Dans cet énoncé,
  - la **variable** x est le sujet de l'énoncé,
  - "est plus grand que 3" est le **prédicat** qui est une propriété que peut avoir le sujet de l'énoncé.

Définition: fonction propositionnelle

Soit toujours l'énoncé

"x est plus grand que 3".

On désigne cet énoncé par $P(x)$ où

- x est la variable,
- P est le prédicat "est plus grand que 3".

On dit alors que l'énoncé $P(x)$ est une **fonction propositionnelle**.

Une fois qu'une valeur est attribuée à la variable x, l'énoncé $P(x)$ devient une proposition et acquiert une valeur de vérité.

Exemple de fonction propositionnelle

Soit l'ensemble $\mathbb{Z}$ des nombres entiers $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.

Soit $P(x)$, la fonction propositionnelle "$x > 0$".

- Cette fonction propositionnelle n'a pas de valeur de vérité tant qu'une valeur n'est pas assignée à la variable x.
- $P(-3)$ est une proposition fausse.
- $P(2)$ est une proposition vraie.
- $P(y) \vee \neg P(0)$ n'est pas une proposition car la variable y n'a pas de valeur.
- $P(3) \vee \neg P(0)$ est une proposition qui est vraie.

Définition: quantification

Spécifier une valeur à une variable permet de transformer une fonction propositionnelle en une proposition.

La **quantification** est une autre méthode pour changer une fonction propositionnelle en une proposition.

On étudiera deux types de quantifications:

- la quantification universelle,
- la quantification existentielle.

Définition: univers du discours

De nombreux énoncés mathématiques affirment qu'une propriété est vraie pour toutes les valeurs d'une variable appartenant à un certain domaine, appelé l'**univers du discours**.

Dans une fonction propositionnelle $P(x)$, l'univers du discours précise les valeurs possibles de la variable x.

Définition: quantification universelle

La **quantification universelle** de $P(x)$ est la proposition

> "$P(x)$ est vraie pour toutes les valeurs de x dans l'univers du discours."

La variable x est limitée à l'univers du discours transformant la fonction propositionnelle $P(x)$ en une proposition.

Définition: quantificateur universel

La notation $\forall x\, P(x)$ désigne la quantification universelle de $P(x)$.

Le symbole $\forall$ est le **quantificateur universel**.

La proposition $\forall x\, P(x)$ s'exprime également

- “pour tout x, $P(x)$”
- “quel que soit x, $P(x)$”.

Exemple de quantification universelle

Lorsqu'il est possible d'énumérer tous les éléments de l'univers du discours, il s'ensuit que la quantification universelle $\forall x\, P(x)$ équivaut logiquement à la conjonction de toutes les propositions de l'univers du discours.

Soit l'univers du discours $U = \{1, 2, 3\}$. Alors

$$\forall x\, P(x) \Leftrightarrow P(1) \wedge P(2) \wedge P(3).$$

Définition: quantification existentielle

La **quantification existentielle** de $P(x)$ est la proposition

> "Il existe un élément x dans l'univers du discours tel que $P(x)$ soit vraie."

La variable x est limitée à l'univers du discours transformant la fonction propositionnelle $P(x)$ en une proposition.

Définition: quantificateur existentiel

La notation $\exists x\, P(x)$ désigne la quantification existentielle de $P(x)$.

Le symbole $\exists$ est le **quantificateur existentiel**.

La proposition $\exists x\, P(x)$ s'exprime également

- "il existe un élément x tel que $P(x)$"
- "il existe au moins un élément x tel que $P(x)$"
- "pour un certain x, $P(x)$".

Exemple de quantification existentielle

Lorsqu'il est possible d'énumérer tous les éléments de l'univers du discours, il s'ensuit que la quantification existentielle $\exists x\, P(x)$ équivaut logiquement à la disjonction de toutes les propositions de l'univers du discours.

Soit l'univers du discours $U = \{1, 2, 3\}$. Alors

$$\exists x\, P(x) \Leftrightarrow P(1) \vee P(2) \vee P(3).$$

Définition: quantification d'existence unique

La **quantification d'existence unique** de $P(x)$ est la proposition

> "Il existe un et un seul élément x dans l'univers du discours tel que $P(x)$ soit vraie."

La variable x est limitée à l'univers du discours transformant la fonction propositionnelle $P(x)$ en une proposition.

Définition: quantificateur d'existence unique

La notation $\exists! x\ P(x)$ désigne la quantification d'existence unique de $P(x)$.

Le symbole $\exists!$ est le **quantificateur d'existence unique**.

La proposition $\exists! x\ P(x)$ s'exprime également

- "il existe un et un seul x tel que $P(x)$"
- "il existe un unique x tel que $P(x)$"
- "on peut trouver seulement un x tel que $P(x)$".

Module Ensembles

Georg Ferdinand Ludwig Philipp Cantor

Né le 3 mars 1845 à St-Petersbourg, Russie.
Mort le 6 janvier 1918 à Halle, Allemagne.

`www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Cantor.html`

Définitions: ensemble et objet

Un **ensemble** est une collection **d'objets**, en nombre fini ou infini, qui possèdent tous la même propriété, celle d'appartenir à l'ensemble.

Les objets qui constituent un ensemble sont également appelés **éléments**, ou **membres**, d'un ensemble. On dit des éléments d'un ensemble qu'ils **appartiennent** à cet ensemble, ou encore que cet ensemble est formé de ses éléments.

Définition: appartenance

On écrit $a \in A$ pour énoncer que a **est un** **élément** **de** (ou **appartient à**) l'ensemble A.

On écrit $a \notin A$ pour énoncer que a **n'est pas un** **élément** **de** (ou **n'appartient pas à**) l'ensemble A.

Représentation des ensembles

Une première manière de représenter un ensemble est de dresser la liste de tous ses éléments et de les mettre entre accolades.

L'ensemble V de toutes les voyelles de l'alphabet français peut s'écrire $V = \{a, e, i, o, u, y\}$.

Représentation des ensembles

On emploie aussi la notation entre accolades pour décrire un ensemble sans en énumérer tous les éléments. On précise les premiers éléments de l'ensemble, puis on insère trois points de suspension (...).

- L'ensemble C de tous les entiers strictement positifs inférieurs à 100 peut s'écrire $C = \{1, 2, 3, ..., 99\}$.
- L'ensemble $\mathbb{N}$ des entiers naturels peut s'écrire $\mathbb{N} = \{0, 1, 2, 3, ...\}$.
- L'ensemble $\mathbb{Z}$ des nombres entiers peut s'écrire $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$.

Représentation des ensembles

On peut décrire un ensemble en utilisant la définition **en compréhension de l'ensemble**. On définit tous les éléments dans l'ensemble en énonçant la ou les propriétés qu'il doivent avoir pour en faire partie.

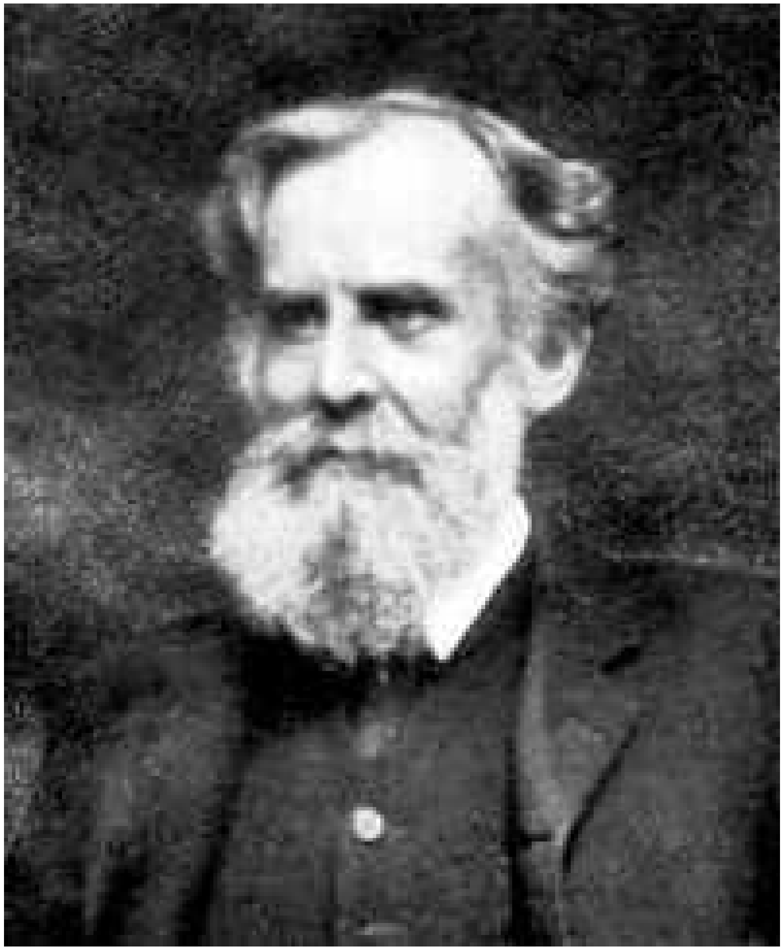
- L'ensemble O de tous les entiers positifs inférieurs à 10 peut s'écrire $O = \{x \,|\, (x \in \mathbb{N}) \wedge (x < 10)\}$.
- L'ensemble $\mathbb{Q}$ de tous les nombres rationnels peut s'écrire $\mathbb{Q} = \{a/b \,|\, (a \in \mathbb{Z}) \wedge (b \in \mathbb{Z}) \wedge (b \neq 0)\}$.

Définition: égalité des ensembles

Deux ensembles sont **égaux** si et seulement s'ils sont formés des mêmes éléments.

Exemple: Les ensembles $\{1, 3, 5\}$ et $\{3, 5, 1\}$ sont égaux.

Note historique: John Venn



Né le 4 août 1834 à Hull, Angleterre.
Mort le 4 avril 1923 à Cambridge, Angleterre.

`www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Venn.h`

Définition: diagramme de Venn

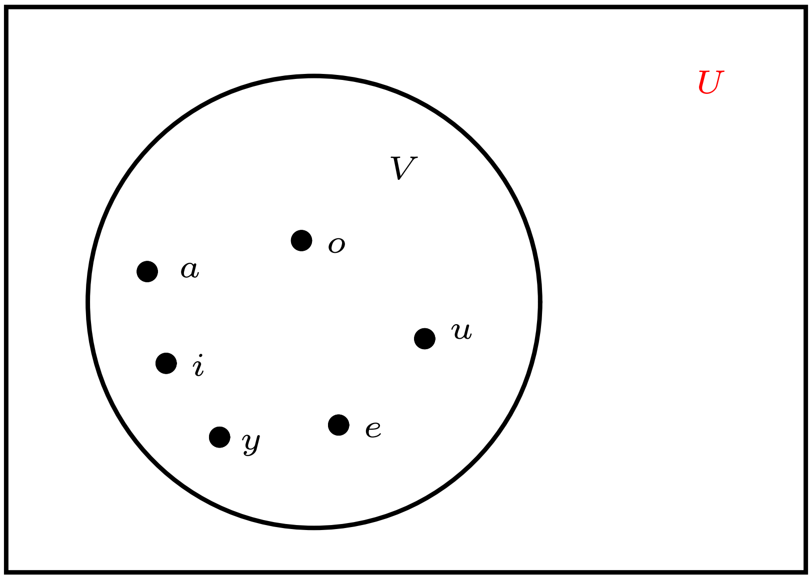
Dans un **diagramme de Venn**, l'**ensemble universel** U, qui contient tous les objets analysés, est représenté par un rectangle.

À l'intérieur de ce rectangle, des cercles ou d'autres figures géométriques servent à représenter les ensembles.

On utilise parfois des points pour symboliser les éléments particuliers d'un ensemble.

Exemple d'un diagramme de Venn

Voici le diagramme de Venn de l'ensemble V des voyelles de l'alphabet français:



Note: Certains auteurs mettent les symboles V et U à l'extérieur du cercle et du rectangle respectivement.

Définition: ensemble vide

Il existe un ensemble spécifique qui ne comporte aucun élément. Cet ensemble est appelé l'**ensemble vide**.

Il est représenté par $\varnothing$ ou encore par $\{\ \}$.

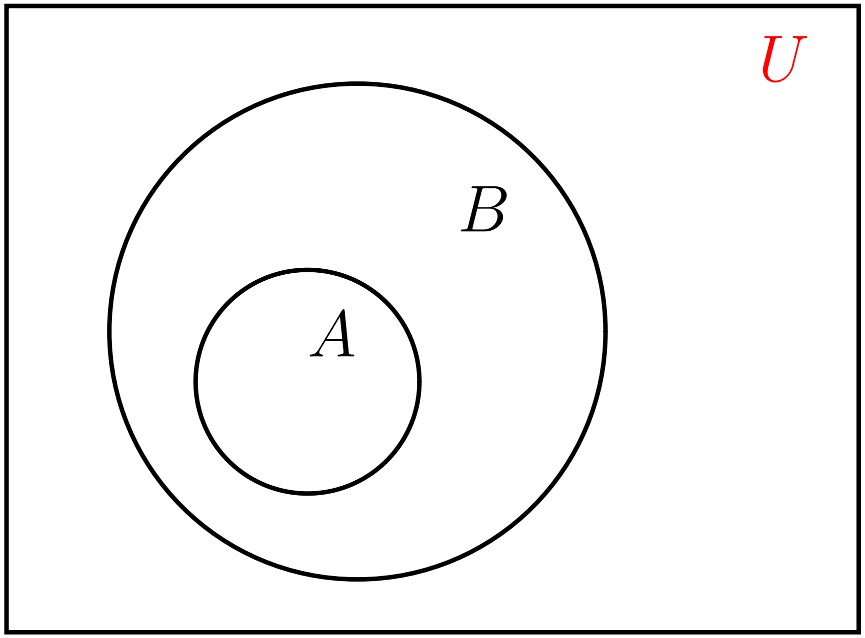
Définition: sous-ensemble

On dit que l'ensemble A est un **sous-ensemble** de l'ensemble B, notée $A \subseteq B$, si et seulement si tous les éléments de A sont également des éléments de B.

- L'ensemble vide est est un sous-ensemble de tous les ensembles, c'est-à-dire, $\varnothing \subseteq S$, quel que soit l'ensemble S.
- Chaque ensemble est un sous-ensemble de lui-même, c'est-à-dire, $S \subseteq S$, quel que soit l'ensemble S.
- Lorsqu'on veut insister sur le fait que l'ensemble A est un sous-ensemble de B, mais que $A \neq B$, on écrit $A \subset B$ et on dit que A est un **sous-ensemble propre** de B. Certains auteurs notent aussi $A \subsetneq B$.

Sous-ensemble

Voici un diagramme de Venn représentant le fait que A est un sous-ensemble de B.



Définition: cardinalité

Soit S, un ensemble. Si S admet exactement n éléments, où n est un entier positif ou nul, on dit que S est un **ensemble fini** et que n est la **cardinalité** de S.

La cardinalité de S est désignée par $|S|$.

On dit qu'un ensemble est **infini** s'il n'est pas fini.

La cardinalité de l'ensemble vide est 0, c.-à-d. $|\varnothing| = 0$.

Définition: puissance d'un ensemble

étant donné un ensemble S, l'**ensemble des parties** de S (ou **puissance** de S) est l'ensemble de tous les sous-ensembles de S. L'ensemble des sous-ensembles de S est noté $P(S)$.

Soit $S = \{0, 1, 2\}$. L'ensemble des parties de S est donné par:
$P(S) =$
$\{\emptyset, \{0\}, \{1\}, \{2\}, \{0, 1\}, \{0, 2\}, \{1, 2\}, \{0, 1, 2\}\}$.

Si $|S| = n$ alors $|P(S)| = 2^n$.

Définition: n-uplet ordonné

Le **n-uplet** $(a_1, a_2, ..., a_n)$ est la collection ordonnée admettant a_1 comme premier élément, a_2 comme deuxième élément, ..., a_n comme n-ième élément.

Deux n-uplets sont égaux si et seulement si les éléments correspondants sont égaux.

On appelle des 2-uplets des **couples** ou des **paires ordonnées**.

Définition: produit cartésien

Soit A et B, deux ensembles. Le **produit cartésien** de A et B, noté $A \times B$, est l'ensemble de tous les couples (a, b), où $a \in A$ et $b \in B$. Ainsi,

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

Exemple: Soit $A = \{1, 2\}$ et $B = \{a, b, c\}$. Alors

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

Note: Les produits cartésiens $A \times B$ et $B \times A$ ne sont pas égaux en général.

Définition: produit cartésien

Le **produit cartésien** des n ensembles A_1, A_2, ..., A_n, noté $A_1 \times A_2 \times \ldots \times A_n$ est l'ensemble des n-uplets $(a_1, a_2, \ldots, a_n)$, où a_i appartient à A_i, pour $i = 1, 2, \ldots, n$. En d'autres termes

$$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i, \text{ pour } i =$$

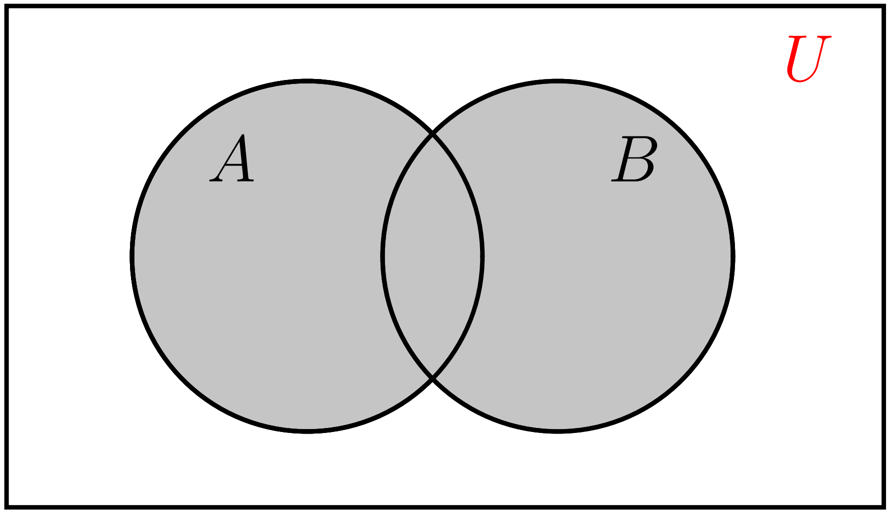
Certains auteurs utilisent la notation

$$A_1 \times A_2 \times \ldots \times A_n = \prod_{i=1}^{n} A_i.$$

Définition: union des ensembles

Soit A et B des ensembles. L'**union** des ensembles A et B, notée $A \cup B$, est l'ensemble qui contient les éléments qui sont soit dans A, soit dans B, ou dans les deux.

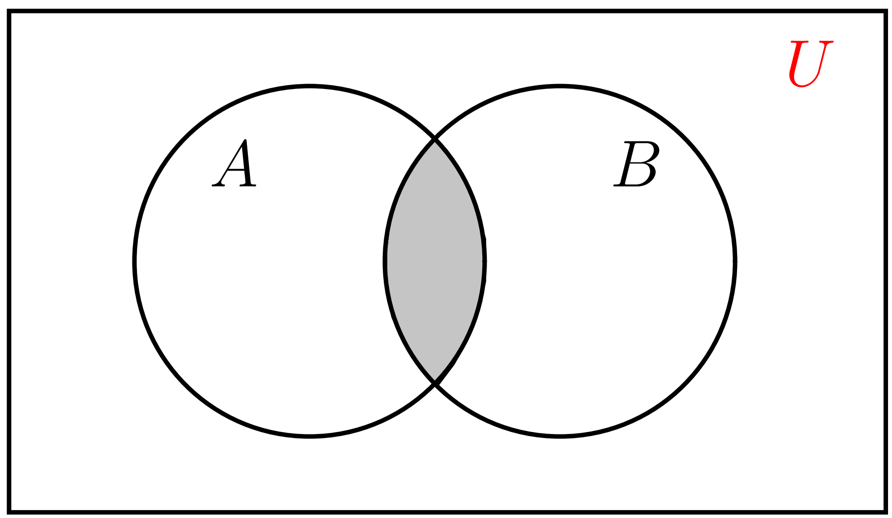
$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$



Définition: intersection des ensembles

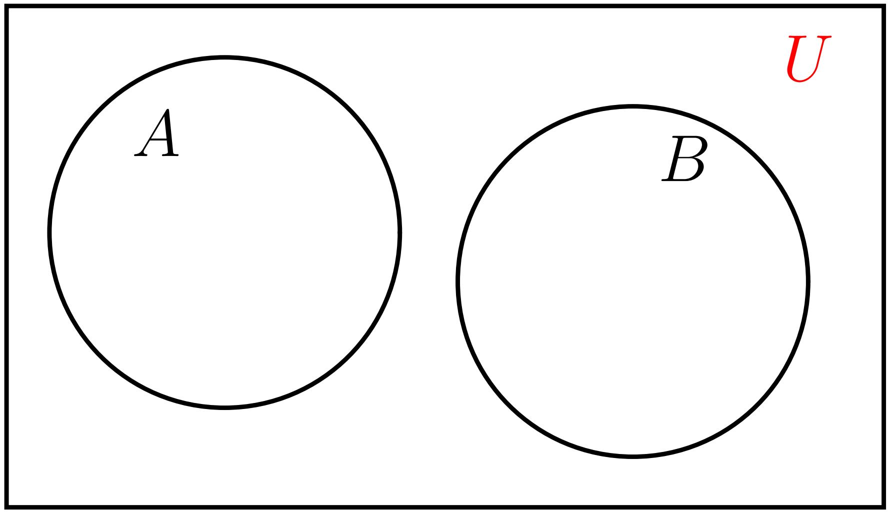
Soit A et B des ensembles. L'**intersection** des ensembles A et B, notée $A \cap B$, est l'ensemble contenant les éléments appartenant à la fois à A et à B.

$$A \cap B = \{x \mid x \in A \wedge x \in B\}.$$



Définition: ensembles disjoints

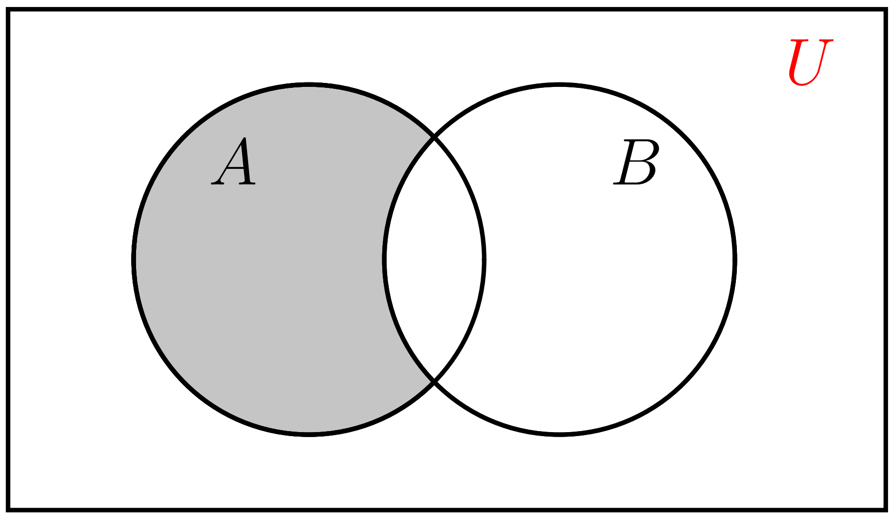
Deux ensembles sont **disjoints** ou **mutuellement exclusifs** si leur intersection est l'ensemble vide.



Définition: différence d'ensembles

Soit A et B des ensembles. La **différence** de A et B, notée $A - B$, est l'ensemble contenant les éléments qui se trouvent dans A mais non dans B.

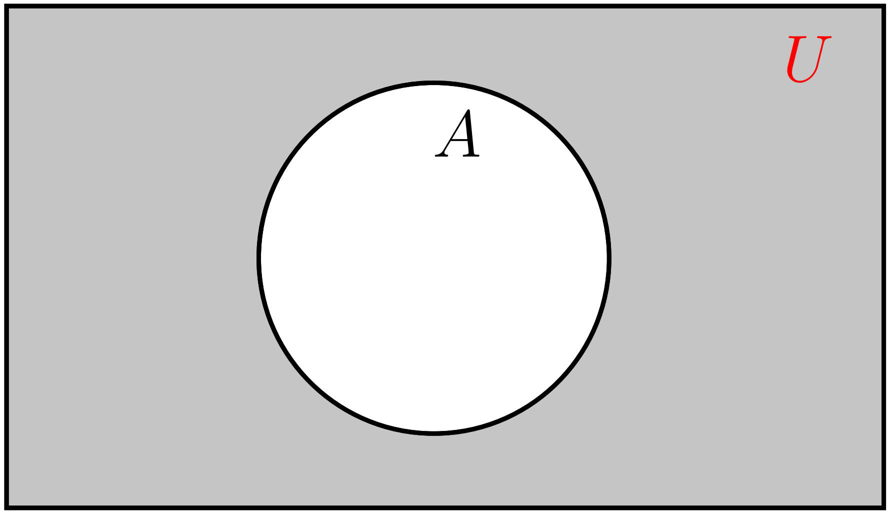
$$A - B = \{x \mid x \in A \wedge x \notin B\}.$$



Définition: complément d'ensembles

Soit U l'ensemble universel. Le **complément** de l'ensemble A, notée $\overline{A}$ ou A^c est l'ensemble des éléments de U qui n'appartiennent pas à A. En d'autres termes, le complément de l'ensemble A est la différence $U - A$.

$$\overline{A} = \{x \mid x \notin A\}.$$



Propriétés des opérations sur les ensembles

Identité	Nom
$A \cup \varnothing = A$ $A \cap U = A$	Identité
$A \cup U = U$ $A \cap \varnothing = \varnothing$	Domination
$A \cup A = A$ $A \cap A = A$	Idempotence
$\overline{(\overline{A})} = A$	Complémentarité

Propriétés des opérations sur les ensembles

Identité	Nom
$A \cup B = B \cup A$ $A \cap B = B \cap A$	Commutativité
$(A \cup B) \cup C = A \cup (B \cup C)$ $(A \cap B) \cap C = A \cap (B \cap C)$	Associativité
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	Distributivité
$\overline{A \cap B} = \overline{A} \cup \overline{B}$ $\overline{A \cup B} = \overline{A} \cap \overline{B}$	Lois de De Morgan

Définition: union généralisée d'ensembles

L'union d'une collection d'ensembles est l'ensemble contenant les éléments qui appartiennent à au moins un ensemble dans la collection.

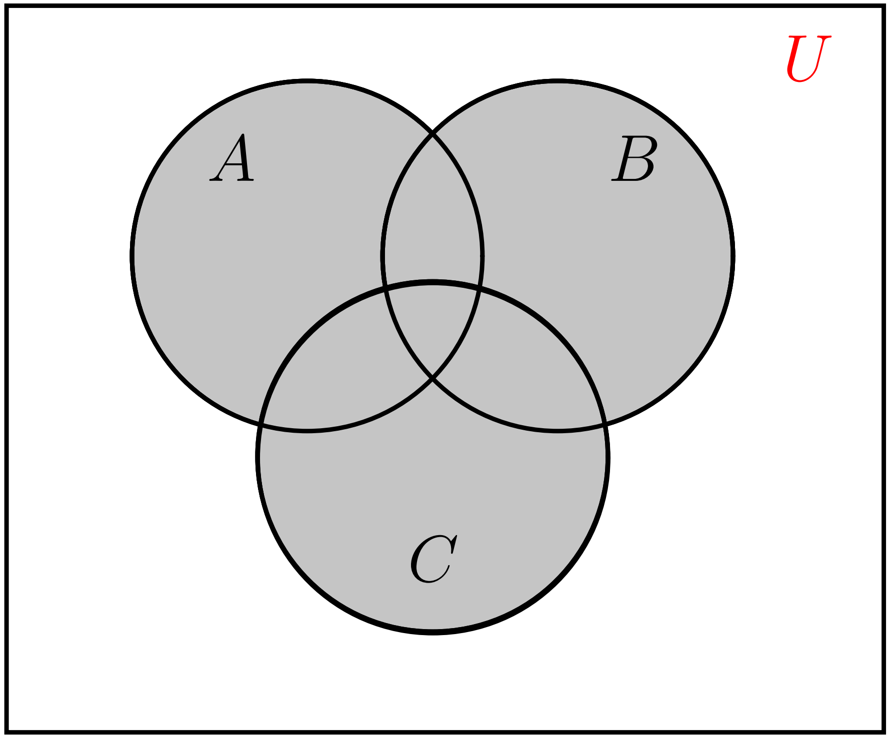
On utilise la notation

$$A_1 \cup A_2 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i$$

pour désigner l'union des ensembles A_1, A_2, ..., A_n.

Exemple d'union généralisée

Ce diagramme de Venn illustre l'union des ensembles A, B et C.



Définition: intersection généralisée d'ensembles

L'intersection d'une collection d'ensembles est l'ensemble contenant les éléments qui appartiennent simultanément à chacun des ensembles.

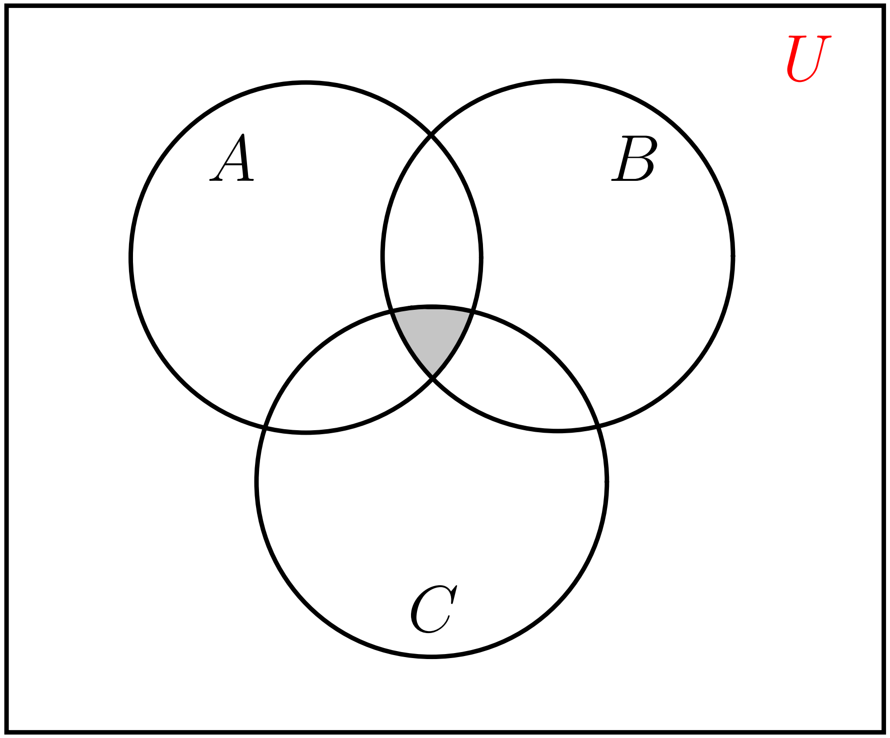
On utilise la notation

$$A_1 \cap A_2 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i$$

pour désigner l'intersection des ensembles $A_1, A_2, \ldots, A_n$.

Exemple d'intersection généralisée

Ce diagramme de Venn illustre l'intersection des ensembles A, B et C.



Raisonnement mathématique : déduction

Méthodes de Preuves

Suite page suivante...

Module: déduction

... suite de la page précédente

raisonnement, théorème et règle d'inférence

- La **démonstration** est la série d'énoncés qui forment le **raisonnement** (ou l'**argumentation**, ou l'**argument**).
- Un **théorème** est un énoncé dont on peut démontrer l'exactitude.
- Une **règle d'inférence** est une règle logique qui permet de déduire les conclusions à partir des hypothèses. Les règles d'inférence relient les étapes d'une démonstration.

Définitions: axiome, lemme, corollaire et conjecture

- Un **axiome** (ou un **postulat**) est un énoncé qui est reconnu pour être vrai.
- Un **lemme** est un “pré-théorème”, ou un théorème simple qu’on utilise pour démontrer d’autres théorèmes.
- Un **corollaire** est un “post-théorème”, ou une proposition qu’on peut établir directement à partir d’un théorème déjà prouvé.
- Une **conjecture** est une proposition qu’on croit vraie mais dont on n’a pas encore trouvé la démonstration.

Définitions: règle d'inférence, hypothèse et conclusion

Certaines tautologies sont des **règles d'inférence**. Elles sont sous la forme

$$(h_1 \wedge h_2 \wedge \ldots \wedge h_n) \rightarrow c$$

où

h_i sont appelés les **hypothèses**

et

c est la **conclusion**.

Notation d'une règle d'inférence

La forme symbolique d'une règle d'inférence est la suivante

$$\frac{h_1, ..., h_n}{c}(r)$$

ou r est le nom de la règle. On dit que la conclusion c est obtenue en appliquant la règle r aux prémisses (hypothèses) $h_1, ..., h_n$.

En général, l'ordre des prémisses ne compte pas.

Règle d'inférence: le *modus ponens*

La règle d'inférence

$$\frac{p \quad p \rightarrow q}{q}(MP)$$

est appelé le ***modus ponens*** (signifie en latin "mode qui affirme") ou **loi de détachement**. Selon le *modus ponens*, si une implication et son hypothèse sont toutes deux vraies, alors la conclusion de cette implication est également vraie.

Le *modus ponens* provient de la tautologie

$$(p \wedge (p \rightarrow q)) \rightarrow q.$$

Exemple de modus ponens

S'il y a du feu, alors il y a de l'oxygène.
Il y a du feu.
Par conséquent, il y a de l'oxygène.

f est la proposition "il y a du feu"
o est la proposition "il y a de l'oxygène"

$$\frac{f \rightarrow o \quad f}{o}(MP)$$

Règle d'inférence : le *modus tollens*

La règle d'inférence

$$\frac{\neg q \quad p \rightarrow q}{\neg p}(MT)$$

est appelé le***modus tollens*** (signifie en latin "mode qui dénie").

Le *modus tollens* provient de la tautologie

$$(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p.$$

Exemple du modus tollens

S'il y a du feu, alors il y a de l'oxygène.
Il n'y a pas d'oxygène.
Par conséquent, il n'y a pas de feu.

f est la proposition "il y a du feu"
o est la proposition "il y a de l'oxygène"

$$\frac{f \rightarrow o \quad \neg o}{\neg f}(MT)$$

Règle d'inférence : l'addition

La règle d'inférence

$$\frac{p}{p \vee q} (Addition)$$

est la règle d'**addition**.

Elle provient de la tautologie

$$p \rightarrow (p \vee q).$$

Règle d'inférence : la simplification

La règle d'inférence

$$\frac{p \wedge q}{p} (Simplification)$$

est la règle de **simplification**.

Elle provient de la tautologie

$$(p \wedge q) \rightarrow p.$$

Règle d'inférence : le syllogisme par hypothèse

La règle d'inférence

$$\frac{p \rightarrow q \quad q \rightarrow r}{p \rightarrow r}(SH)$$

est la règle du **syllogisme par hypothèse** (syllogisme signifie "raisonnement formé de trois propositions dont la dernière, la conclusion, est nécessairement vraie si les deux premières, les hypothèses, sont admises").

Elle provient de la tautologie

$$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r).$$

Règle d'inférence : le syllogisme disjonctif

La règle d'inférence

$$\frac{p \vee q \qquad \neg p}{q}\,(SD)$$

est la règle du **syllogisme disjonctif**.

Elle provient de la tautologie

$$(p \vee q) \wedge \neg p \rightarrow q.$$

Règle d'inférence : la conjonction

La règle d'inférence

$$\frac{p \quad q}{p \land q}(Conjonction)$$

est la règle de **conjonction**.

Elle provient de la tautologie

$$(p \land q) \to (p \land q).$$

Règle d'inférence : le dilemme constructif

La règle d'inférence

$$\frac{(p \rightarrow q) \wedge (r \rightarrow s) \quad p \vee r}{q \vee s}(DilemmeConstructif)$$

est la règle du **dilemme constructif**.

Elle provient de la tautologie

$$(((p \rightarrow q) \wedge (r \rightarrow s)) \wedge (p \vee r)) \rightarrow (q \vee s).$$

Définition: contrevérités

- Les **contrevérités** sont des raisonnements inexacts.
- Les contrevérités ressemblent aux règles d'inférence, mais elles sont fondées sur des contingences plutôt que sur des tautologies.

Contrevérité d'affirmer la conclusion

La "règle d'inférence"

$$\frac{p \rightarrow q \quad q}{p}$$

est une contrevérité (et donc n'est plus une règle d'inférence à proprement parler).

Elle provient de la contingence

$$((p \rightarrow q) \wedge q) \rightarrow p$$

qui n'est pas une tautologie.

Exemple de contrevérité

S'il y a du feu, alors il y a de l'oxygène.
Il y a de l'oxygène.
Par conséquent, il y a du feu?

f est la proposition "il y a du feu"
o est la proposition "il y a de l'oxygène"

$$\frac{f \rightarrow o \quad o}{f}$$

ce qui, à partir des hypothèses, est une conclusion fausse.

Contrevérité d'ignorer l'hypothèse

La "règles d'inférence"

$$\frac{p \rightarrow q \qquad \neg p}{\neg q}$$

est une contrevérité (et donc n'est plus une règle d'inférence à proprement parler).

Elle provient de la contingence

$$((p \rightarrow q) \wedge \neg p) \rightarrow \neg q$$

qui n'est pas une tautologie.

Exemple de contrevérité

S'il y a du feu, alors il y a de l'oxygène.
Il n'y a pas de feu.
Par conséquent, il n'y a pas d'oxygène.

f est la proposition "il y a du feu"
o est la proposition "il y a de l'oxygène"

$$\frac{f \rightarrow o \qquad \neg f}{\neg o}$$

ce qui, à partir des hypothèses, est une conclusion fausse.

Exemple de preuve formelle

Considérons le raisonnement suivant:

Si les chevaux volent ou les vaches mangent des artichauts, alors le maringouin est l'oiseau national. Si le maringouin est l'oiseau national, alors le beurre de peanut est bon sur des hot-dogs. Mais, le beurre de peanut est abject sur des hot-dogs.

Par conséquent, les vaches ne mangent pas d'artichauts.

Exemple de preuve formelle (suite)

Désignons les propositions composant le raisonnement par des lettres:

- c est “les **c**hevaux volent”
- v est “les **v**aches mangent des artichauts”
- m est “le **m**aringouin est l’oiseau national”
- b est “le **b**eurre de peanut est bon sur des hot-dogs”

On représente le raisonnement formel à l’aide des variables

$$\frac{h_1.\ (c \vee v) \rightarrow m \quad h_2.\ m \rightarrow b \quad h_3.\ \neg b}{\neg v} ???$$

Exemple d'une preuve formelle (suite)

Construction de la preuve

1.	$(c \lor v) \to m$	h_1
2.	$m \to b$	h_2
3.	$(c \lor v) \to b$	étapes 1 et 2 et règle du syllogisme par hypothèse.
4.	$\neg b$	h_3
5.	$\neg(c \lor v)$	étapes 3 et 4 et règle du *modus tollens*.
6.	$\neg c \land \neg v$	étape 5 et loi de De Morgan
7.	$\neg v$	étape 6 et règle de simplification.

C. Q. F. D., Q. E. D. ou $\blacksquare$

Les méthodes de preuve

Pour établir la vérité de l'implication $p \to q$, où p peut être une conjonction d'autres hypothèses, on dispose de plusieurs méthodes:

- preuve triviale,
- preuve vide,
- preuve directe,
- preuve indirecte,
- preuve par l'absurde,
- preuve cas par cas.

Preuve triviale

Si on sait que la conclusion q est vraie, alors l'implication $p \rightarrow q$ est vrai quelque soit la valeur de vérité de p.

Exemple:
S'il pleut aujourd'hui, alors l'ensemble vide est un sous-ensemble de tous les ensembles.

À noter que l'hypothèse n'est pas nécessaire dans la démonstration.

Preuve vide

Si on sait que l'hypothèse p de l'implication $p \to q$ est fausse, alors l'implication est toujours vraie.

Exemple:
Si je suis à la fois riche et pauvre, alors Superman existe.

Si l'hypothèse est fausse, on peut conclure n'importe quoi.

Preuve directe

On suppose que p est vraie et on utilise les règles d'inférence et des théorèmes déjà démontrés pour prouver que q doit être également vraie.

Exemple:
Voir l'exemple de la preuve "*les vaches ne mangent pas d'artichauts.*"

Preuve indirecte

La preuve indirecte est la preuve directe de la contraposée. Puisque l'implication $p \rightarrow q$ est logiquement équivalent à sa contraposée $\neg q \rightarrow \neg p$, on peut prouver l'implication en démontrant que sa contraposée est vraie.

Exemple:
Pour prouver que

"*Si* $3n + 2$ *est impair, alors* n *est impair,*"

on présume que n est pair et on en déduit que $3n + 2$ est pair.

Preuve par l'absurde

Pour prouver une proposition p, on suppose qu'elle est fausse, et que cela entraîne une contradiction, c.-à-d. $\neg p \to \mathrm{F}$. On en conclut qu'elle est vraie.

Note 1: Une contradiction est en général de la forme $r \wedge \neg r$.

Note 2: Dans le cas où la proposition à démontrer est l'implication $p \to q$, supposer qu'elle est fausse revient à supposer que la proposition $\neg(p \to q)$ est vraie, que $\neg(\neg p \vee q)$ est vraie, et donc que $p \wedge \neg q$ est vraie.

Preuve cas par cas

Lorsque l'hypothèse peut s'écrire sous la forme de cas

$$p_1 \vee p_2 \vee \ldots \vee p_n,$$

alors montrer l'implication

$$(p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q$$

est équivalent à montrer

$$(p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge (p_n \rightarrow q).$$

Cette méthode de preuve provient de la tautologie

$$((p_1 \vee p_2 \vee \ldots \vee p_n) \rightarrow q) \Leftrightarrow ((p_1 \rightarrow q) \wedge (p_2 \rightarrow q) \wedge \ldots \wedge ($$

Contrevérité par raisonnement circulaire

Cela arrive quand on utilise le fait que la conclusion est vraie dans la preuve elle-même.

Exemple:

Conjecture: *Si x^2 est pair, alors x est pair.*
Note: Cette conjecture est vraie, mais la preuve qui suit est fausse.
Preuve circulaire: *Si x^2 est pair, alors il existe un k tel que $x^2 = 2k$. Alors il existe un l tel que $x = 2l$. Par conséquent, x est pair.*

Règles d'inférence pour les quantificateurs

Il y a quatre règles d'inférence pour les quantificateurs:

- l'instantiation universelle (IU),
- la généralisation universelle (GU),
- l'instantiation existentielle (IE),
- la généralisation existentielle (GE).

L'instantiation universelle

$$\frac{\forall x\, P(x)}{\therefore\ P(c)}$$

$$\frac{\forall x\, P(x)}{P(c)}(IU)$$

Si une fonction propositionnelle est vraie pour tout élément de l'univers du discours, alors elle est vraie pour un élément particulier, arbitraire ou non, de l'univers du discours.

L'instantiation universelle – Exemple

Tous les hommes ont deux jambes. Pierre Tremblay est un homme. Par conséquent Pierre Tremblay a deux jambes.

Définissons les prédicats:

- $H(x)$ est "x est un homme"
- $J(x)$ est "x a deux jambes"
- t est "Pierre Tremblay", un élément de l'univers du discours.

Le raisonnement devient:

$$\begin{array}{l} 1.\ \forall x\,(H(x) \rightarrow J(x)) \\ 2.\ H(t) \\ \hline \therefore\ J(t) \end{array}$$

L'instantiation universelle – Exemple (suite)

Construction de la preuve

1.	$\forall x\,(H(x) \to J(x))$	Hypothèse h_1
2.	$H(t) \to J(t)$	étape 1 et IU
3.	$H(t)$	Hypothèse h_2
4.	$J(t)$	étape 2 et 3 et *modus ponens*

$\blacksquare$

La généralisation universelle

$$\frac{P(x)}{\therefore\ \forall x\, P(x)}$$

$$\frac{P(x)}{\forall x\, P(x)}(GU)$$

Il y a tout un cadre formel pour que cette règle puisse s'appliquer. Brièvement, il faut définir un univers du discours. Ensuite, il faut vérifier la validité de la fonction propositionnelle $P(x)$ pour un x, de l'univers du discours, arbitraire, quelconque, un x sur lequel on a fait aucune hypothèse restrictive. Si tel est le cas, alors $P(x)$ est vraie pour tout x de l'univers du discours.

L'instantiation existentielle

$$\frac{\exists x\, P(x)}{\therefore\ P(c)}$$

$$\frac{\exists x\, P(x)}{P(c)}(IE)$$

Dans cette règle, c n'est pas n'importe quel élément x de l'univers du discours, c doit être un élément de l'univers du discours pour lequel $P(x)$ est vraie.

La généralisation existentielle

$$\frac{P(c)}{\therefore\ \exists x\, P(x)}$$

$$\frac{P(c)}{\exists x\, P(x)}(GE)$$

Si une fonction propositionnelle $P(x)$ est vraie pour un élément c de l'univers du discours, alors on peut affirmer qu'il existe un x de l'univers du discours tel que la fonction propositionnelle $P(x)$ est vraie.

Les méthodes de preuve d'existence

- Preuve d'existence constructive
- Preuve d'existence non constructive
- Preuve de non existence par contre-exemple

Preuve d'existence constructive

Pour prouver que $\exists x \, P(x)$,

- on trouve un élément c de l'univers du discours pour lequel $P(c)$ est vraie.
- Alors, $\exists x \, P(x)$ est vraie par généralisation existentielle.

Exemple:
THÉORÈME: *Il existe une solution entière à l'équation* $x^2 + y^2 = z^2$.
Esquisse de la preuve: Choisir $x = 3$, $y = 4$ et $z = 5$.

Preuve d'existence non constructive

On peut prouver que $\exists x\, P(x)$ sans construire un élément c tel que $P(c)$ est vraie. La preuve d'existence est dite non constructive.

Pour cela on peut utiliser la preuve par l'absurde et démontrer que la négation de la quantification existentielle implique une contradiction.

Preuve de non existence par contre-exemple

Pour prouver que $\neg\exists x\, P(x)$ (qui est équivalent à $\forall x\, \neg P(x)$), on peut utiliser une preuve par l'absurde. On suppose qu'il existe un c tel que $P(c)$ et on en déduit une contradiction.

Preuve de non existence de Superman

Si Superman voulait et pouvait prévenir le mal, il le ferait. Si Superman était incapable de prévenir le mal, il serait impuissant; s'il ne voulait pas prévenir le mal, il serait malveillant. Superman ne prévient pas le mal. Si Superman existe, il n'est ni impuissant ni malveillant. Donc, Superman n'existe pas.

Preuve de non existence de Superman

Définissons les propositions:

- v est “Superman **v**eut prévenir le mal”
- p est “Superman **p**eut prévenir le mal”
- i est “Superman est **i**mpuissant”
- m est “Superman est **m**alveillant”
- r est “Superman p**r**évient le mal”
- x est “Superman e**x**iste”

Preuve de non existence de Superman

Définissons les hypothèses:

- h_1. $(v \wedge p) \to r$
- h_2. $\neg p \to i$
- h_3. $\neg v \to m$
- h_4. $\neg r$
- h_5. $x \to \neg i$
- h_6. $x \to \neg m$

Preuve de non existence de Superman

Construction de la preuve

1.	$\neg i \rightarrow p$	contraposée de h_2
2.	$x \rightarrow p$	h_5 et étape 1 avec syll. par hyp.
3.	$\neg m \rightarrow v$	contraposée de h_3
4.	$x \rightarrow v$	h_6 et étape 3 avec syll. par hyp.
5.	$x \rightarrow (p \wedge v)$	étape 2 et 4 par conjonction
6.	$x \rightarrow r$	étape 5 et h_1 avec syll. par hyp.
7.	$\neg x$	étape 6 et h_4 par *modus tollens*

$\blacksquare$

Module Relations

Relations et propriété

Suite page suivante...

Module Relation

... suite de la page précédente

Module Classes d'équivalence et partitions (144)

- Relation d'équivalence (144) • Classe d'équivalence (145)
- Partition (147)
- Combinaison de Relations (150)

Module Ordre partiel et ordre total (151)

- Relation d'ordre (151)
- Ordre total (154)

Définition: relation binaire

Soit A et B deux ensembles. Une **relation binaire** de A à B est un sous-ensemble de $A \times B$.

Exemple: Soit $A = \{0, 1, 2\}$ et $B = \{a, b\}$. Alors $R = \{(0, a), (0, b), (1, a), (2, b)\} \subseteq A \times B$ est une relation de A à B.

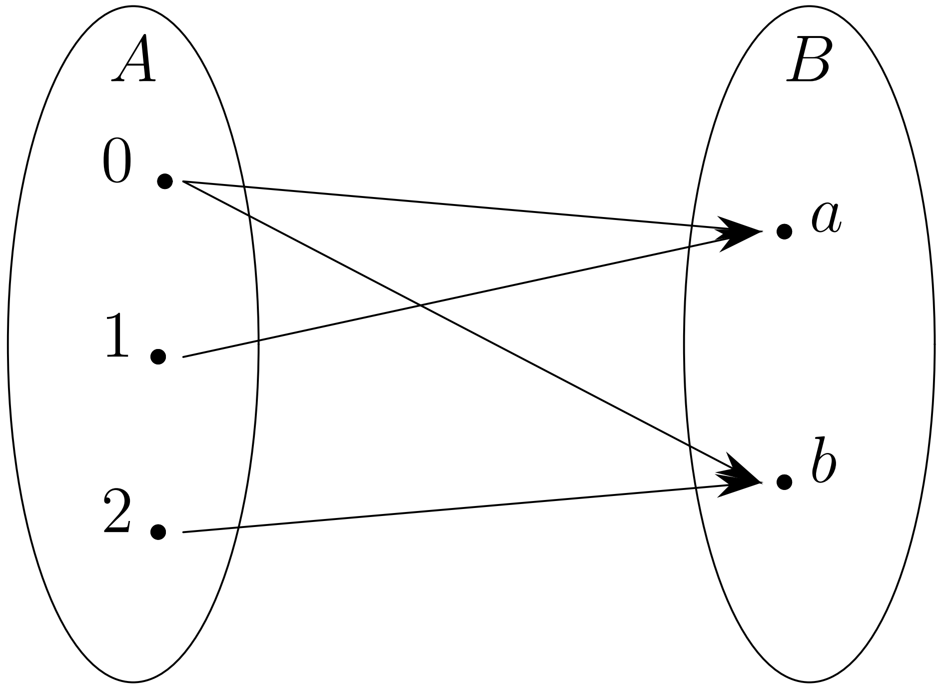
En d'autre termes, une relation binaire de A à B est un ensemble R de couples, où le premier élément de chaque couple provient de A et le deuxième élément, de B. On a recours à la notation $a\,R\,b$ pour indiquer que $(a, b) \in R$ et à la notation $a \not{R}\, b$ pour indiquer que $(a, b) \notin R$. De plus, lorsque $(a, b) \in R$, on dit que a est en relation avec b par R.

Représentation à l'aide d'un graphe orienté

Un **graphe orienté** est constitué d'un ensemble V de **sommets** et d'un ensemble E de couples d'éléments de V appelés des **arcs**. On appelle le sommet a le **sommet initial** de l'arc (a, b) et le sommet b, le **sommet final** de cet arc.

Exemple d'un graphe orienté

Exemple: Soit $A = \{0, 1, 2\}$, $B = \{a, b\}$ et la relation $R = \{(0, a), (0, b), (1, a), (2, b)\}$ de A à B.



Représentation à l'aide d'un tableau

Soit R, une relation binaire de A à B. Les lignes du tableau de la relation sont l'énumération des éléments de l'ensemble A et les colonnes, de l'ensemble B. Il y a un $\times$ à une certaine ligne et une certaine colonne de ce tableau si l'élément correspondant de cette ligne est en relation à l'élément correspondant de cette colonne.

Exemple du tableau d'une relation

Exemple: Soit $A = \{0, 1, 2\}$, $B = \{a, b\}$ et la relation $R = \{(0, a), (0, b), (1, a), (2, b)\}$ de A à B.

R	a	b
0	$\times$	$\times$
1	$\times$	
2		$\times$

Note: Un tableau est ni plus ni moins qu'une matrice.

Représentation matricielle d'une relation

On suppose que R est une relation de $A = \{a_1, a_2, ..., a_m\}$ et $B = \{b_1, b_2, ..., b_n\}$. Ici, les éléments des ensembles A et B ont été énumérés dans un ordre particulier mais arbitraire. De plus, lorsque $A = B$, on utilise le même ordre pour A et B. On peut représenter la relation R à l'aide de la matrice $\mathbf{M}_R = [m_{ij}]$, où

$$m_{ij} = \begin{cases} 1 & \text{si } (a_i, b_j) \in R, \\ 0 & \text{si } (a_i, b_j) \notin R, \end{cases}$$

Exemple de représentation matricielle

Exemple: Soit $A = \{0, 1, 2\}$, $B = \{a, b\}$ et la relation $R = \{(0, a), (0, b), (1, a), (2, b)\}$ de A à B.

$$\mathbf{M}_R = \begin{array}{c c} & \begin{array}{cc} a & b \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \end{array} & \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} \end{array} .$$

Définition: relation dans un ensemble

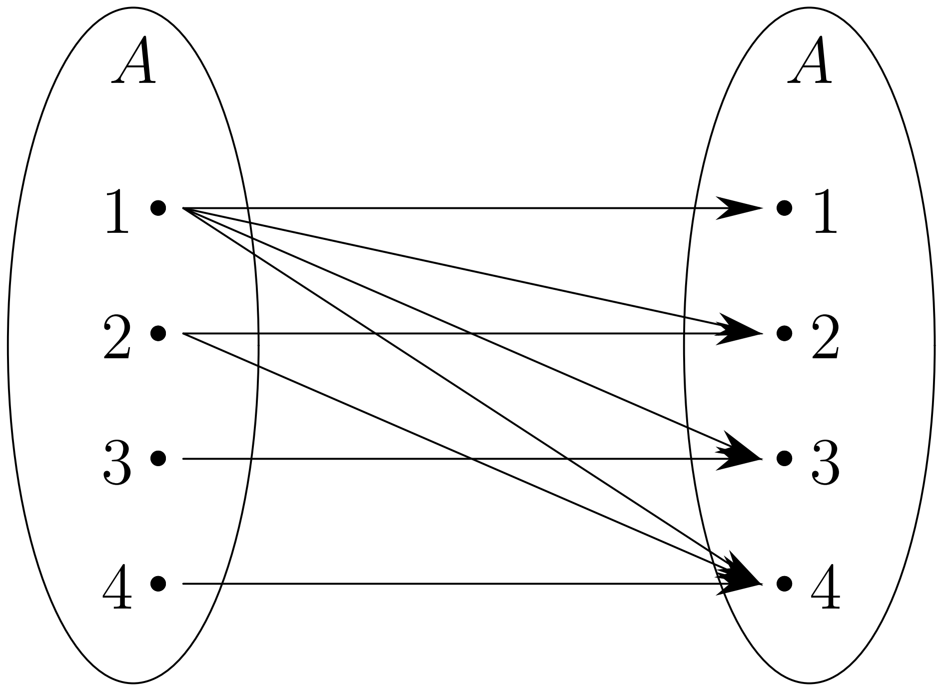
Une **relation dans un ensemble** A est une relation entre A et A.

Exemple: Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(a, b) \,|\, a \text{ divise } b\} \subseteq A \times A$.

Les couples de cette relation sont donnés par
$R =$
$\{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.

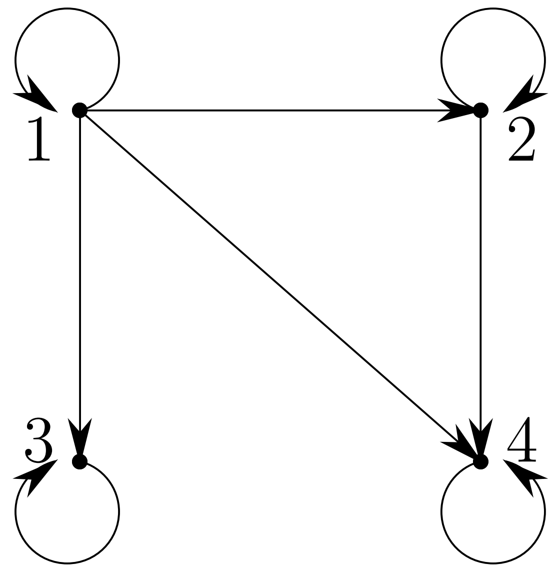
Représentation à l'aide d'un graphe orienté

Soit $A = \{1, 2, 3, 4\}$. Soit la relation $R = \{(a, b) \mid a \text{ divise } b\}$. $R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,4), (3,3), (4,4)\}$.



Représentation à l'aide d'un graphe orienté

Soit $A = \{1, 2, 3, 4\}$. Soit la relation $R = \{(a, b) \mid a \text{ divise } b\}$. $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.



On représente un arc de la forme (a, a) à l'aide d'une **boucle**.

Représentation à l'aide d'un tableau

Soit $A = \{1, 2, 3, 4\}$. Soit la relation $R = \{(a, b) \mid a \text{ divise } b\}$. $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.

R	1	2	3	4
1	$\times$	$\times$	$\times$	$\times$
2		$\times$		$\times$
3			$\times$	
4				$\times$

Représentation matricielle d’une relation

Soit $A = \{1, 2, 3, 4\}$. Soit la relation $R = \{(a, b) \mid a$ divise $b\}$. $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 4), (3, 3), (4, 4)\}$.

$$\mathbf{M}_R = \begin{array}{cc} & \begin{array}{cccc} 1 & 2 & 3 & 4 \end{array} \\ \begin{array}{c} 1 \\ 2 \\ 3 \\ 4 \end{array} & \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \end{array}.$$

Définition: relation réflexive

Une relation R dans un ensemble A est dite **réflexive** si $(a, a) \in R$ pour tout élément $a \in A$.

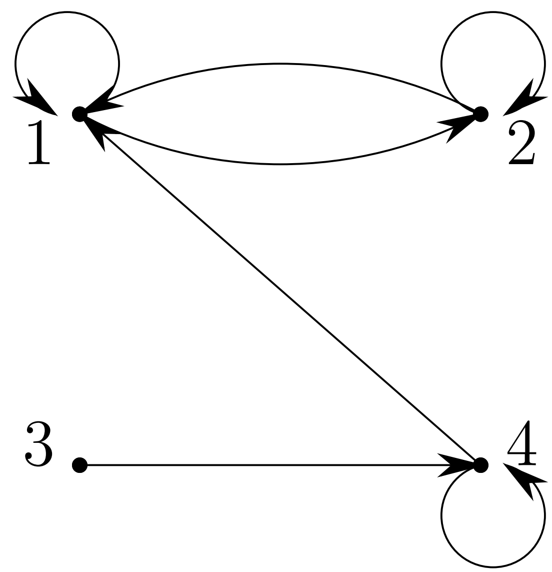
Exemple: Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation
$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$.
Cette relation est-elle réflexive?

Non, car il manque

(3, 3)

Représentation à l'aide d'un graphe orienté

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation
$R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$.
Cette relation est-elle réflexive?



Représentation matricielle d'une relation

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1),(1,2),(2,1),(2,2),(3,4),(4,1),(4,4)\}$.
Cette relation est-elle réflexive?

Non, car pas de 1 sur sa diagonale

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Définition: relation symétrique

Une relation R dans un ensemble A est **symétrique** si $(a, b) \in R$ implique que $(b, a) \in R$ pour tout $a, b \in R$.

Exemple: Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation
$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$.
Cette relation est-elle symétrique?

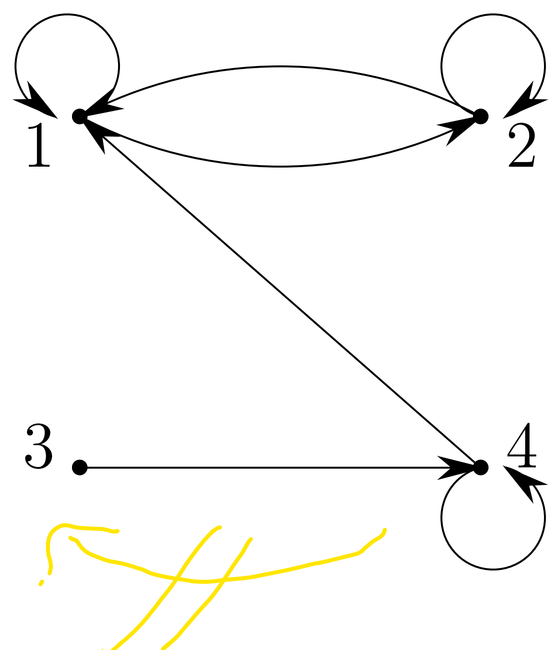
Non, car pas de

$(4, 3)$ $(1, 4)$

Représentation à l'aide d'un graphe orienté

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$. Cette relation est-elle symétrique?

Non, car
Pour un chemin d'aller je dois avoir un retour



Représentation matricielle d'une relation

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$. Cette relation est-elle symétrique?

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Non car doit être 1 et 1

Définition: relation anti-symétrique

Une relation R dans un ensemble A est **antisymétrique** si $(a, b) \in R$ et $(b, a) \in R$ si et seulement si $a = b$ pour tout $a, b \in R$.

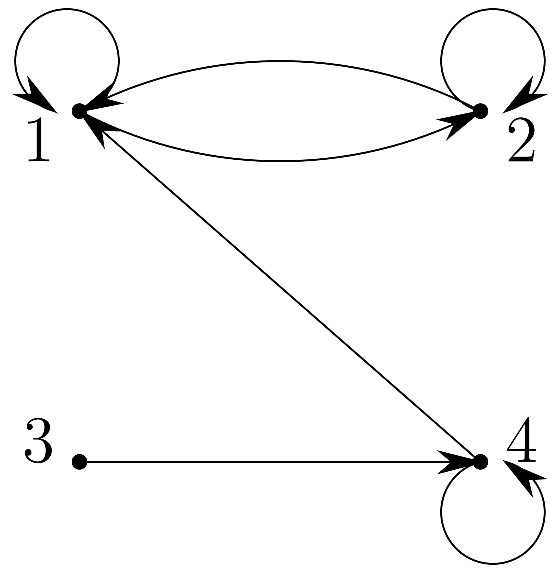
Exemple: Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation
$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$.
Cette relation est-elle antisymétrique?

Non, car 1 est différent de 2

Représentation à l'aide d'un graphe orienté

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$. Cette relation est-elle antisymétrique?

Non



Représentation matricielle d'une relation

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$. Cette relation est-elle antisymétrique?

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Définition: relation transitive

Une relation R dans un ensemble S est **transitive** si, lorsque $(a, b) \in R$ et $(b, c) \in R$, alors $(a, c) \in R$ pour tout $a, b, c \in R$.

Exemple: Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation
$R = \{(1, 1), (1, 2), (2, 1), (2, 2), \boxed{(3, 4)}, (4, 1), (4, 4)\}$.
Cette relation est-elle transitive?

Non

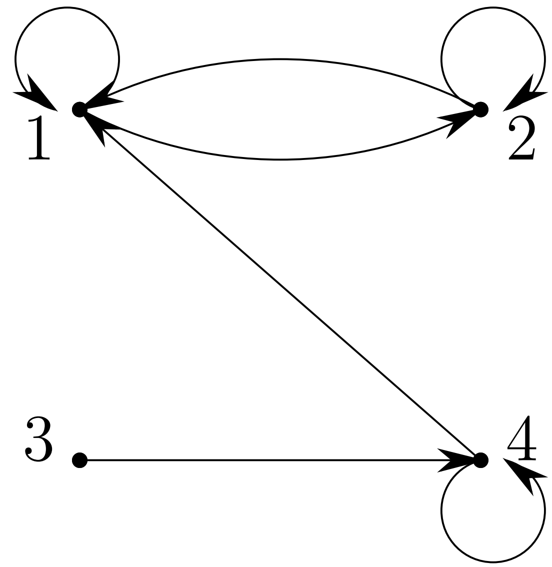
Je commence par les (,) débutant par 4

Pas de (3, 1)

donc ∅ transitive

Représentation à l'aide d'un graphe orienté

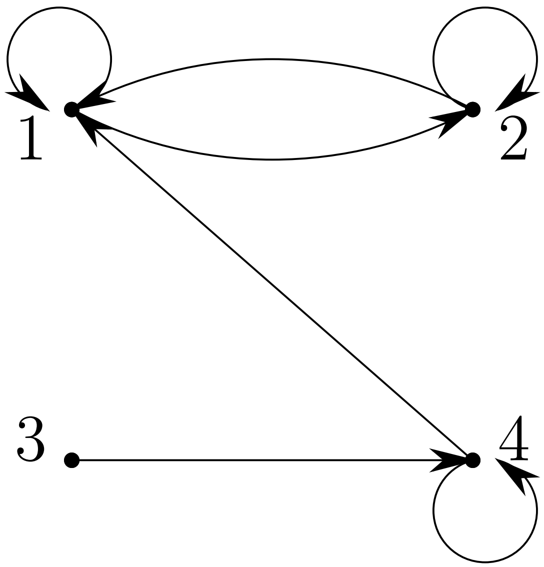
Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$. Cette relation est-elle transitive?

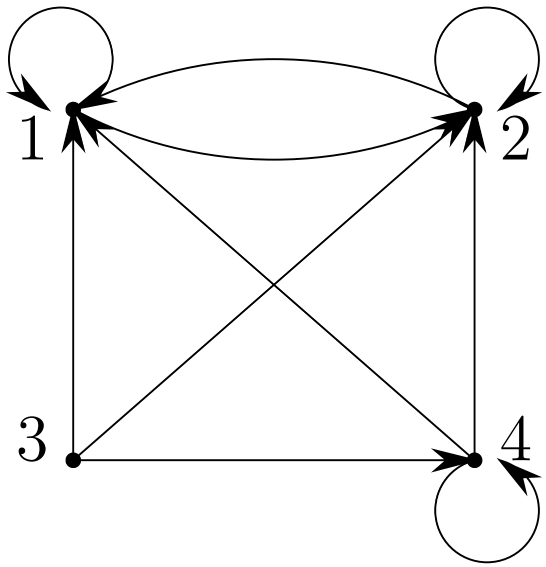


Non car il manque le chemin (3,1)

Représentation à l'aide d'un graphe orienté

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$. Cette relation est-elle transitive?





Il faut fermer les "chemins triangulaires".

Représentation matricielle d’une relation

Soit A l’ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 4), (4, 1), (4, 4)\}$. Cette relation est-elle transitive?

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Représentation matricielle d'une relation

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$. Cette relation est-elle transitive?

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

La méthode pour obtenir une relation transitive n'est pas évidente (voir Chapitre sur les fermetures page 225).

Définition: relation d'équivalence

Voir document sur équivalences

Une relation dans un ensemble A est une **relation d'équivalence** si elle est réflexive, symétrique et transitive.

Deux éléments reliés par le biais d'une relation d'équivalence sont **équivalents**. Exemple:

On dit que a **est congru à** b **modulo** m si m divise $a - b$. Notation: $a \equiv b \pmod m$. La relation

$$R = \{(a, b) \,|\, a \equiv b \pmod m\}$$

est une relation d'équivalence dans l'ensemble des entiers.

Définition: classe d'équivalence

Soit R, une relation d'équivalence dans un ensemble A. L'ensemble des éléments qui sont en relation avec un élément a de A est appelé la **classe d'équivalence** de a et elle est notée $[a]_R$. Lorsqu'on ne considère qu'une seule relation, on supprime l'indice R et on écrit $[a]$ pour cette classe d'équivalence.

En d'autres mots, si R est une relation d'équivalence dans un ensemble A, la classe d'équivalence de a est

$$[a]_R = \{s \in A \mid (a, s) \in R\}.$$

Si $b \in [a]_R$, on appelle b un **représentant** de cette classe d'équivalence.

Classe d'équivalence

THÉORÈME: Soit R une relation d'équivalence dans un ensemble A. Les énoncés suivants sont équivalents:

i) $a\,R\,b$, → a en relation avec b

ii) $[a] = [b]$, → b appartient à la classe de a } Symétrique

iii) $[a] \cap [b] \neq \emptyset$.

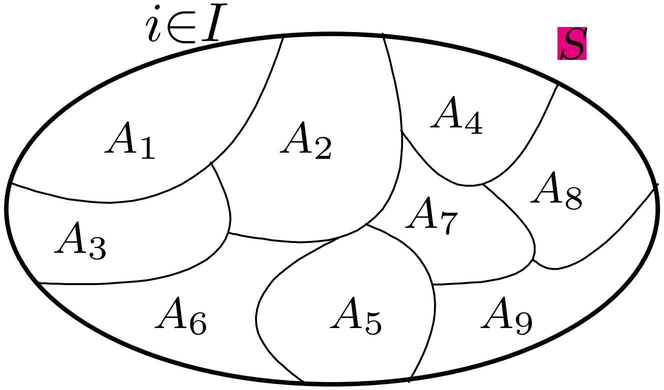
DÉMONSTRATION:
$i) \implies ii)$ Par définition
$ii) \implies iii)$ trivial
$iii) \implies i)$ $\exists x \in [a]$ and $x \in [b]$. Donc xRa et xRb. Ce qui implique $a \in [x]$ et $b \in [x]$. Par conséquent aRb.

Définition: partition

Une **partition** d'un ensemble S est un ensemble de sous-ensembles disjoints et non vides de S qui ont S comme union.

En d'autres mots, l'ensemble des sous-ensembles A_i, $i \in I$ (où I est un ensemble d'indices) forme une partition de S si et seulement si

- $A_i \neq \emptyset \quad \forall i \in I$,
- $A_i \cap A_j = \emptyset$, pour $i \neq j$,
- $\bigcup_{i \in I} A_i = S$.



Partition induite

THÉORÈME: Soit R une relation d'équivalence dans un ensemble S, Alors, les classes d'équivalence de R forment une partition de S.

Inversement, étant donné une partition $\{A_i \mid i \in I\}$ de l'ensemble S, il existe une relation d'équivalence R qui admet les ensembles A_i, $i \in I$ comme classes d'équivalence.

Démonstration page suivante...

Partition induite: démonstration

- $\Rightarrow$
  - Les classes sont non vides (à cause de la réfléxivité)
  - 2 classes qui ont un élément commun sont égales:
    Soit $c \in [a]$ et $c \in [b]$; donc aRc et bRc. Soit $x \in [a]$ on a aRx. Or aRc et $aRx \Rightarrow cRx$ et bRc et $cRx \Rightarrow bRx$. Donc $x \in [b]$.
    Tout élément de $[a]$ est élément de $[b]$.
    On peut faire le même raisonnement pour un élément de $[b]$. Donc $[a] = [b]$.
- $\Leftarrow$ Soit une partition de A. On définit la relation R par "xRy quand x et y appartiennent à la même composante de la partition". C'est une relation d'équivalence et la classe de x est la composante qui contient x.

Combinaison de relations

On peut combiner deux relations entre A et B comme on peut combiner deux ensembles puisque les relations entre A et B sont des sous-ensembles du produit cartésien $A \times B$.

Exemple: $A = \{1, 2, 3\}$, $b = \{1, 2, 3, 4\}$. Les relations $R_1 = \{(1, 1), (2, 2), (3, 3)\}$ et $R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4)\}$ se combinent pour obtenir

- $R_1 \cup R_2 = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3)\}$.
- $R_1 \cap R_2 = \{(1, 1)\}$.
- $R_1 - R_2 = \{(2, 2), (3, 3)\}$.
- $R_2 - R_1 = \{(1, 2), (1, 3), (1, 4)\}$.

Définition: Relation d'ordre

Une relation R dans un ensemble S est appelée une **relation de préordre** ou d'**ordre partiel** si elle est réflexive, antisymétrique et transitive.

Un ensemble S combiné à une relation de préordre R est appelé un **ensemble partiellement ordonné** et est noté (S, R).

Exemples

- Soit l'ensemble $S = \{1, 2, 3, 4, 6\}$ et la relation $R = \{(a, b) \in S \times S \mid a|b\}$. Divisibilité
- Soit l'ensemble $S = \{1, 2, 3, 4\}$ et la relation $R = \{(a, b) \in S \times S \mid a \leq b\}$.

Antisymétrie

$(a,b) \wedge (b,a) \rightarrow a=b$

ex: $4/2$ $2/4$ Non

$(6/6) \wedge (6/6) \longrightarrow 6=6$

R : en relation

Notation

(S, R)

Dans un ensemble partiellement ordonné, la notation $a \preccurlyeq b$ signifie que $(a, b) \in R$. a R b

La notation $a \prec b$ symbolise que $a \preccurlyeq b$, mais que $a \neq b$. De plus, on dit que “a est plus petit que b” si $a \prec b$.

Les éléments a et b d’un ensemble partiellement ordonné $(S, \preccurlyeq)$ sont **comparables** si soit $a \preccurlyeq b$, soit $b \preccurlyeq a$.

Lorsque a et b sont des éléments de S, de manière telle que ni $a \preccurlyeq b$ ni $b \preccurlyeq a$, alors a et b sont **incomparables**.

Définition: ordre total

Si $(S, \preccurlyeq)$ est un ensemble partiellement ordonné et que tous les deux éléments quelconques de S sont comparables, alors S est appelé un **ensemble totalement ordonné** et $\preccurlyeq$, un $\boxed{\textbf{ordre total}}$. Un ensemble totalement ordonné est également appelé une **chaîne**.

(S, R) $(S, \leq)$

- ordre partiel
- les éléments 2 à 2 comparables

Module Fonctions

Fonctions

Suite page suivante...

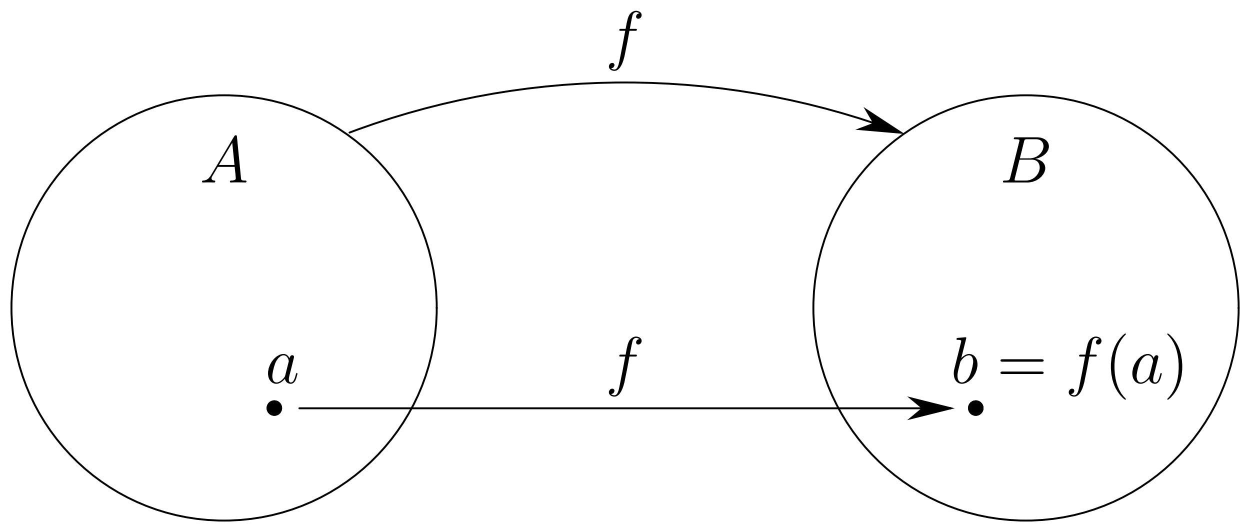
Module Fonctions

... suite de la page précédente

Définition: fonction

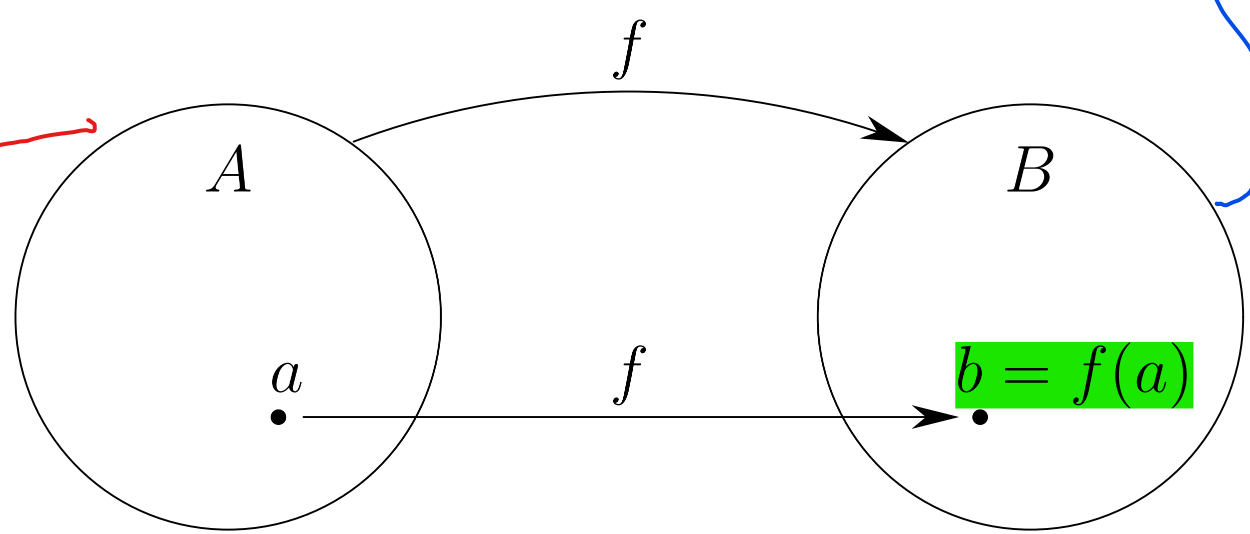
Soit A et B, deux ensembles. On appelle **fonction** f de A dans B l'affectation d'*au plus un* élément de B à chaque élément de A. On écrit $f(a) = b$ si b est le *seul* élément de B attribué par la fonction f à l'élément a de A. Si f est une fonction de A dans B, on écrit $f : A \to B$. Lorsqu'une fonction affecte a chaque élément de A *exactement* un élément de B, elle est appelée **application**.

Pas plus que 1 ex:



codomaine, image et préimage

Si f est une fonction de A dans B, on dit que A est le **domaine** de f et B, le **codomaine** de f. Si $f(a) = b$, on dit que b est **l'image** de a et que a est la antécédent **préimage** de b. La **portée** de f est l'ensemble de toutes les images des éléments de A. De même, si f est une fonction de A dans B, on dit que f fait **correspondre** A à B.

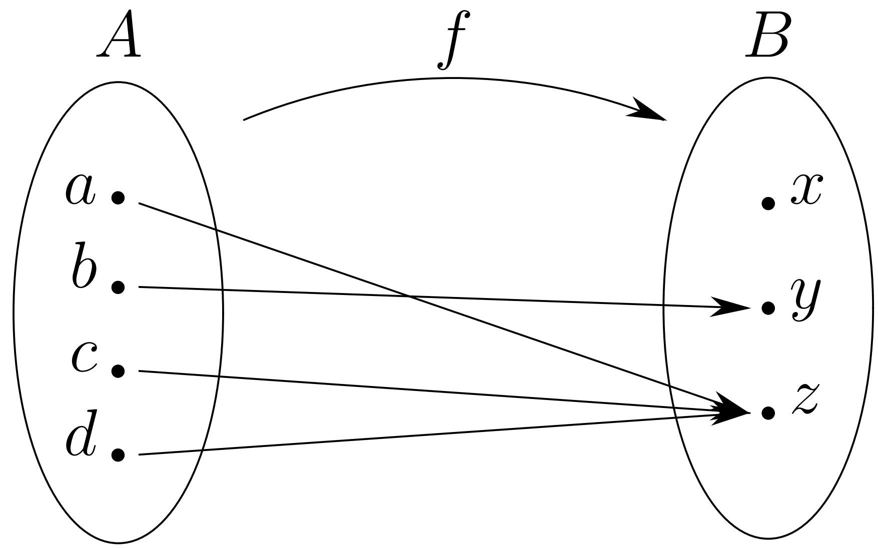


Définition: image d'un sous-ensemble

Soit f une fonction de l'ensemble A dans l'ensemble B et soit S, un sous-ensemble de A. **L'image** de S est un sous-ensemble de B qui comprend les images des éléments de S. On désigne l'image de S par $f(S)$. Ainsi,

$$f(S) = \{f(s) \mid s \in S\}.$$

Exemple



- Le domaine de f est $A = \{a, b, c, d\}$.
- Le codomaine de f est $B = \{x, y, z\}$.
- $f(a) = z$.
- L'image de a est z.
- Les préimages de z sont a, c et d.

Définition: fonction injective, surjectve, bijective

Les propriétés d'une fonction

Une fonction f est **injective** si et seulement si $f(x) = f(y)$ implique que $x = y$ pour toutes les valeurs de x et y dans le domaine de f. On appelle cette application une **injection**.

Dit d'une autre façon, par la contraposée, une fonction f est **injective** si et seulement si $x \neq y$ implique que $f(x) \neq f(y)$.

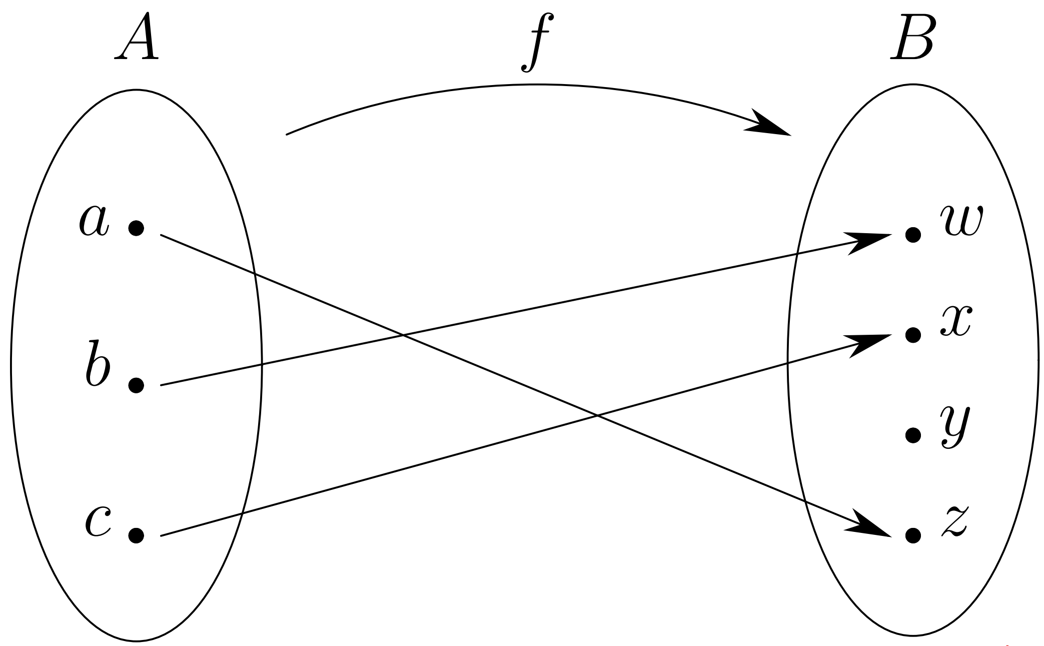
Portée = Codomaine !

La fonction f de A dans B est **surjective** si et seulement si, pour chaque élément de $b \in B$ dans le codomaine, il existe un élément $a \in A$ tel que $f(a) = b$. On appelle cette application une **surjection**.

b est son image

On dit qu'une fonction f est **bijective**, ou encore que c'est une **bijection**, si f est à la fois injective et surjective.

Exemple 1



Est-ce que f est injectif? Oui, car chaque élément de A a des images differents

Est-ce que f est surjectif? Non

▷ y n'est pas dans la portée

- Une fonction? Oui car chaque élément de B a au plus 1 élément de A

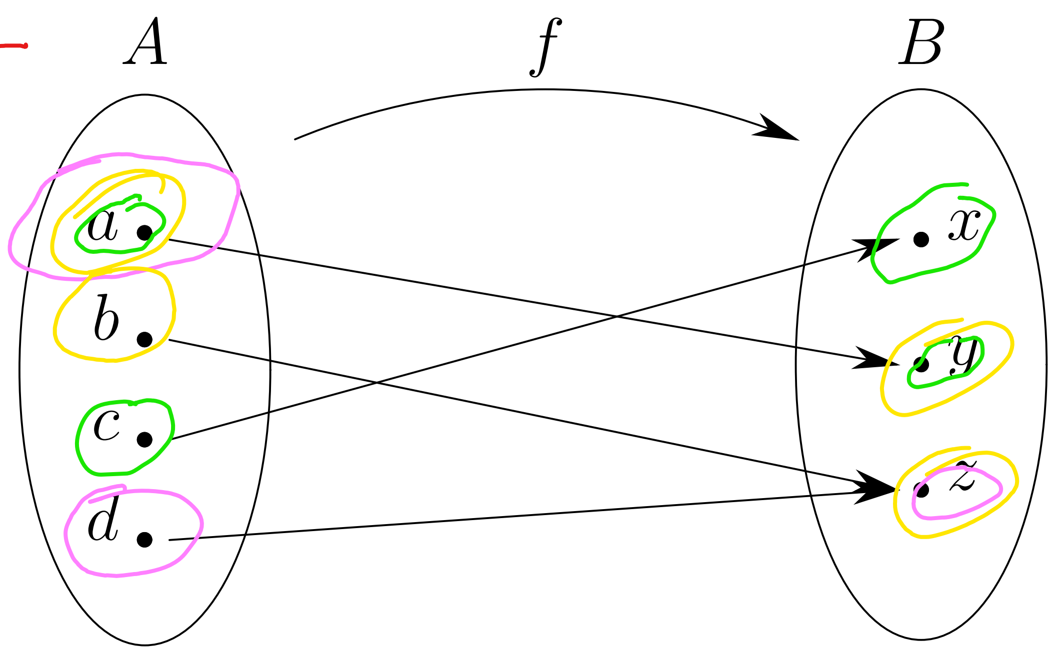
Exemple 2

Différents?

a et b ✓
a et c ✓
a et d ✓

b et c ✓
b et d ✗

⇒ donc Pas Injectif



Est-ce que f est injectif? Non

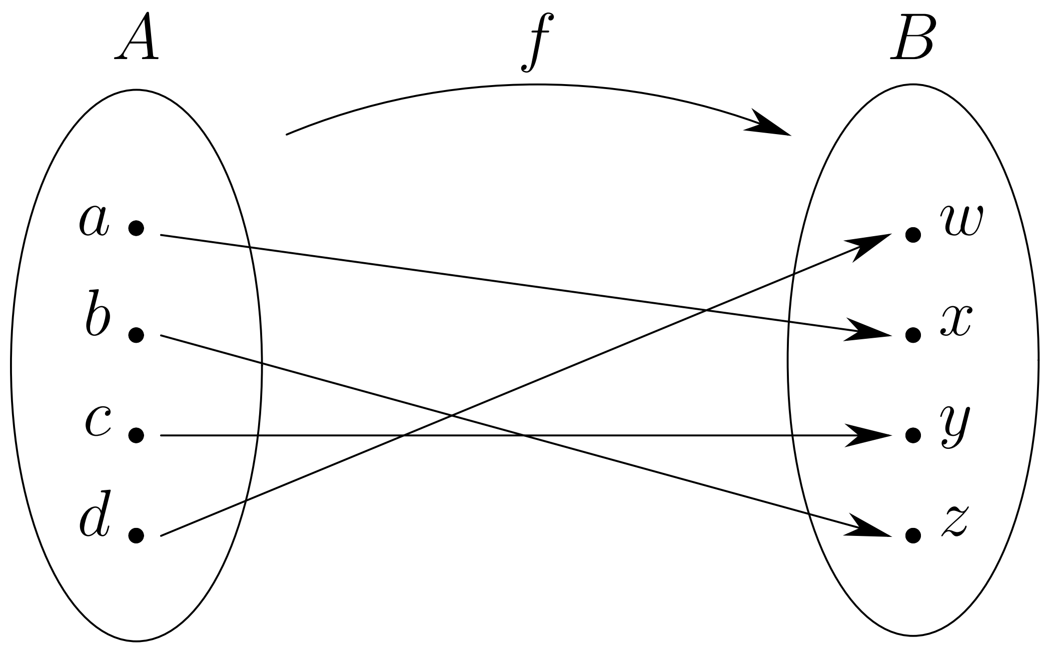
Est-ce que f est surjectif?

Oui con

Portée x, y, z = B? Oui, on tout est associé

donc surjectif

Exemple 3

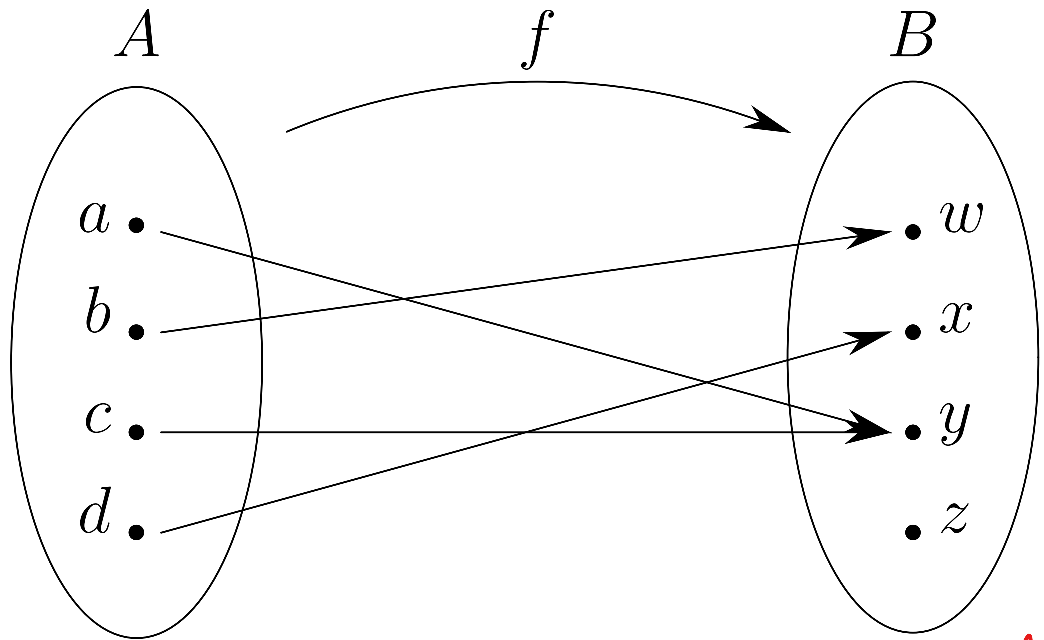


Est-ce que f est injectif? Oui

Est-ce que f est surjectif? Oui

Surjectif car aucun élément de B est laissé seul

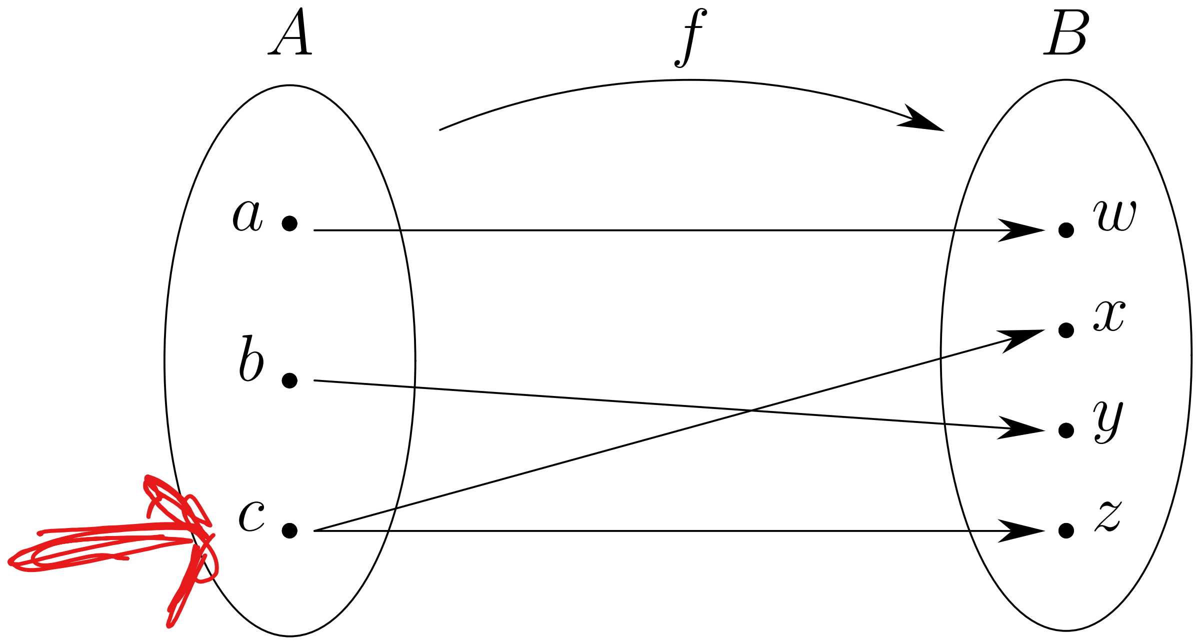
Exemple 4



Est-ce que f est injectif? Non, car a et c à y

Est-ce que f est surjectif? Non, car z est pas associé à rien

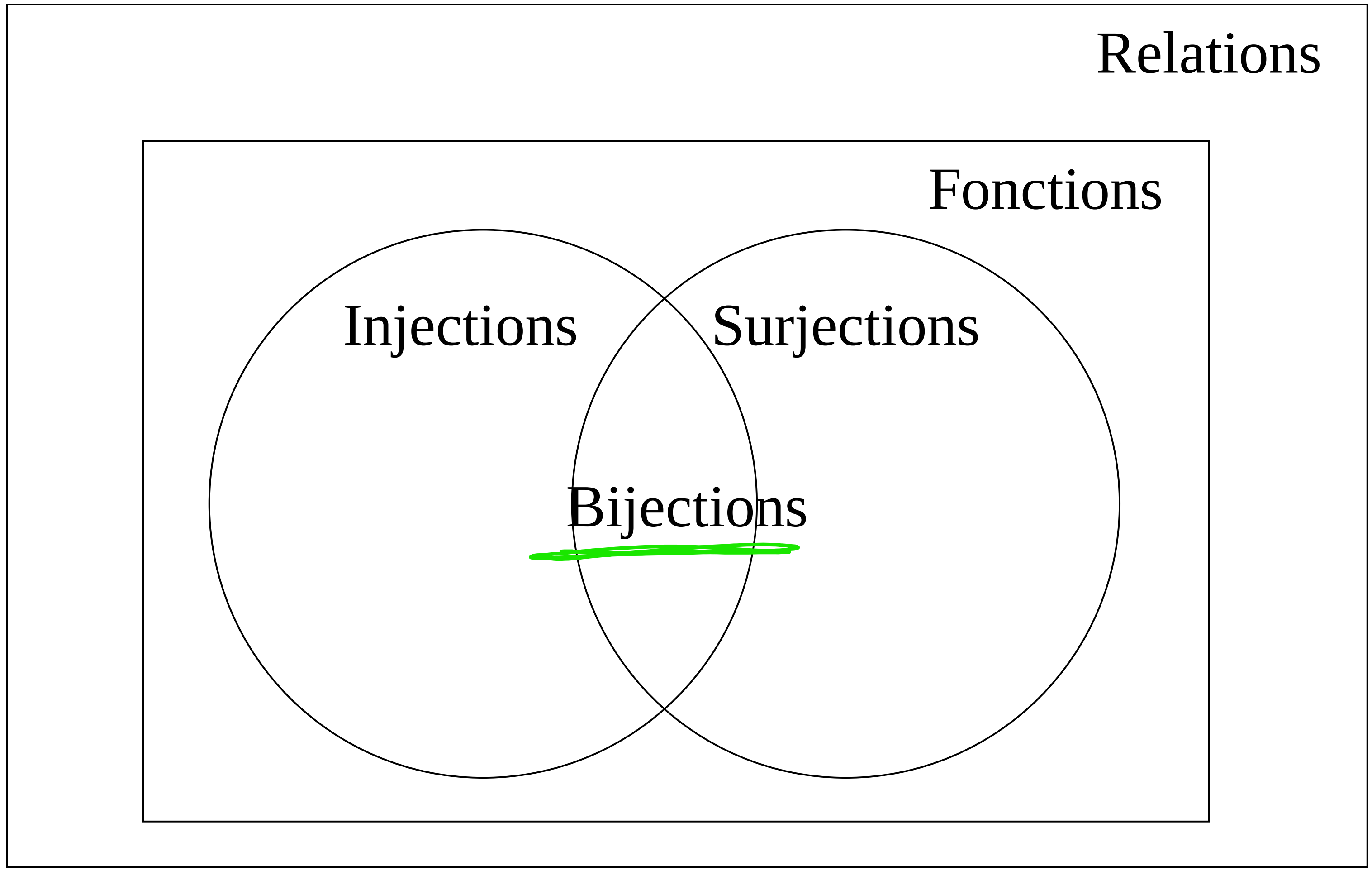
Exemple 5



Est-ce que f est injectif?
Est-ce que f est surjectif?

Pas une fonction

Diagramme de Venn de classification des fonctions



Définition: cardinalité - Ensembles Dénombrables

La définition de la bijection permet d'introduire de nouvelles propriétés des ensembles: Les ensembles A

et B sont de même **cardinalité** si et seulement si il existe une bijection de A dans B.

Définition : Un ensemble E est dit *dénombrable* quand il est *équipotent* à l'ensemble des entiers naturels $\mathbb{N}$, c'est-à-dire qu'il existe une bijection de $\mathbb{N}$ sur E. A contrario, un ensemble (infini) *non dénombrable*, est un ensemble infini qui n'est pas équipotent à $\mathbb{N}$.

Exemples d'ensembles Dénombrables

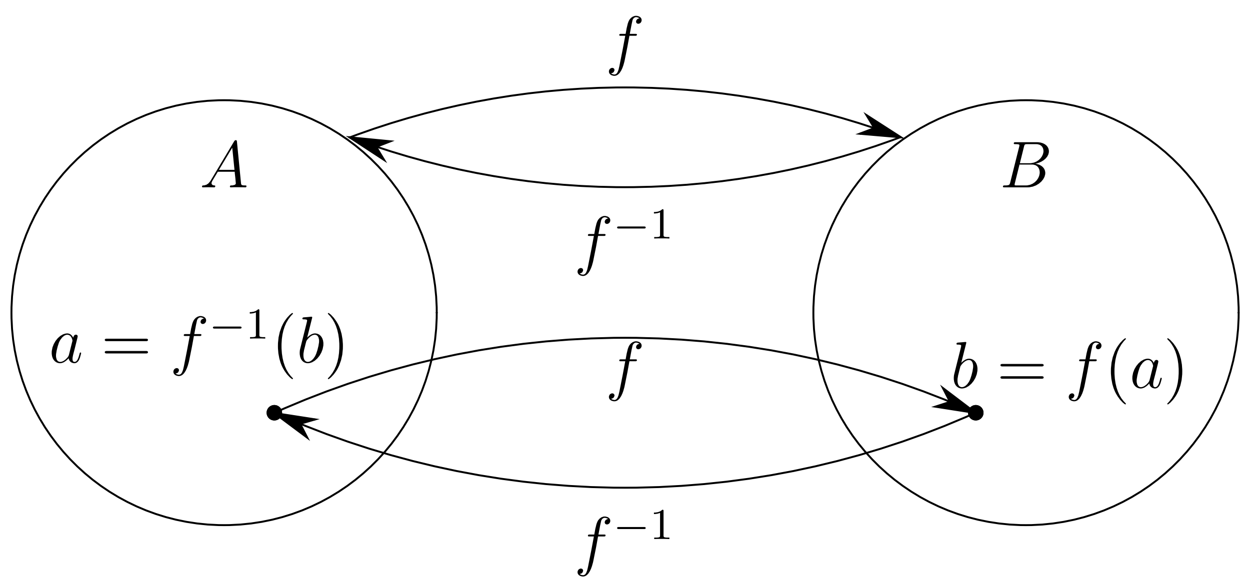
Exemples :

- L'ensemble $\mathbb{N}$ des entiers naturels est bien sûr dénombrable par définition, mais, on peut démontrer que chacun de ses sous-ensembles infinis l'est également.
- l'ensemble des nombres premiers est dénombrable.
- On peut montrer que l'ensemble des réels et l'ensemble des parties de $\mathbb{N}$ ne sont pas dénombrables (diagonale de Cantor).

D'abord bijective

Définition: fonction inverse

Soit f, une bijection de l'ensemble A dans l'ensemble B. La **fonction inverse** de f est la fonction qui associe à un élément b appartenant à B un unique élément a appartenant à A tel que $f(a) = b$. La fonction inverse de f est représentée par f^{-1}. Dans ce cas, $f^{-1}(b) = a$ quand $f(a) = b$. La fonction inverse est aussi une bijection.

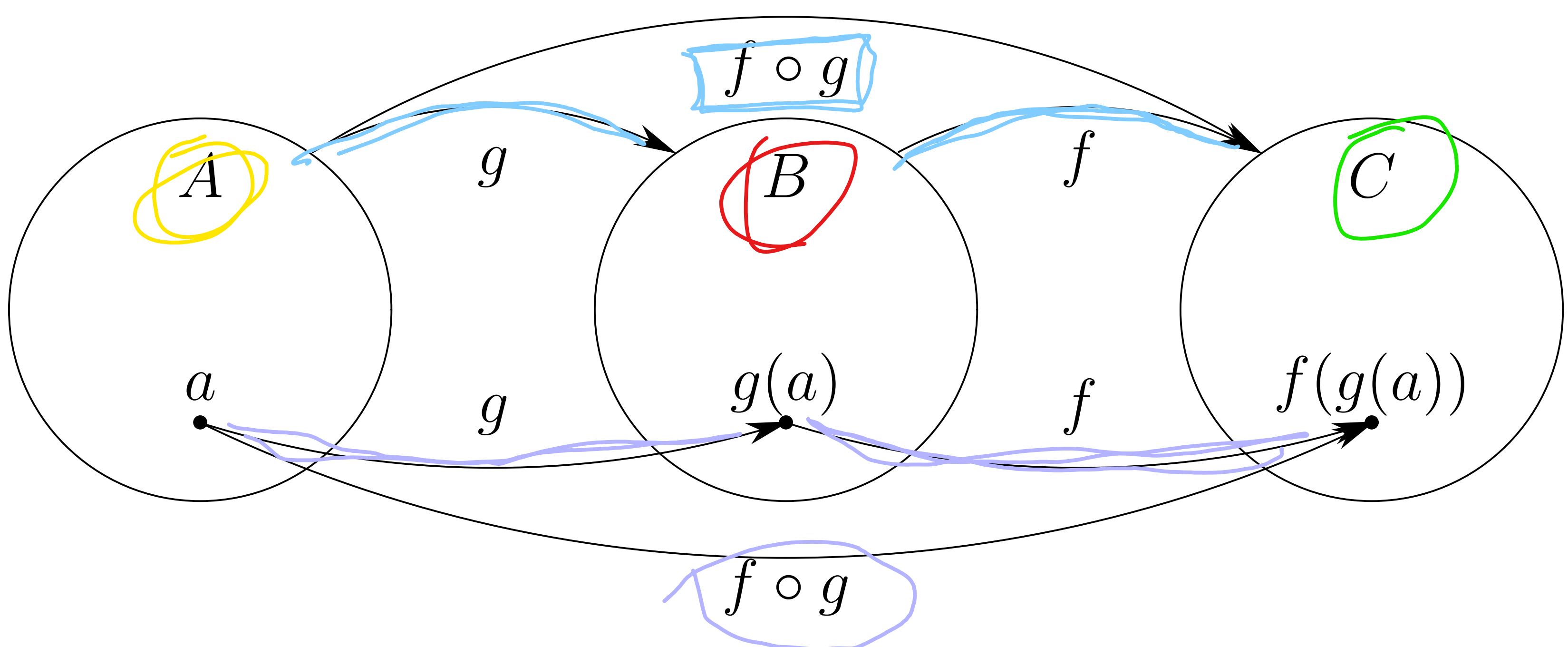


Définition: composition de fonctions

Soit g une fonction de l'ensemble A dans l'ensemble B, et soit f, une fonction de l'ensemble B dans l'ensemble C. La **composition des fonctions** f et g, représentée par $f \circ g$, est définie par

rond

$$\boxed{(f \circ g)(a) = f(g(a)).}$$

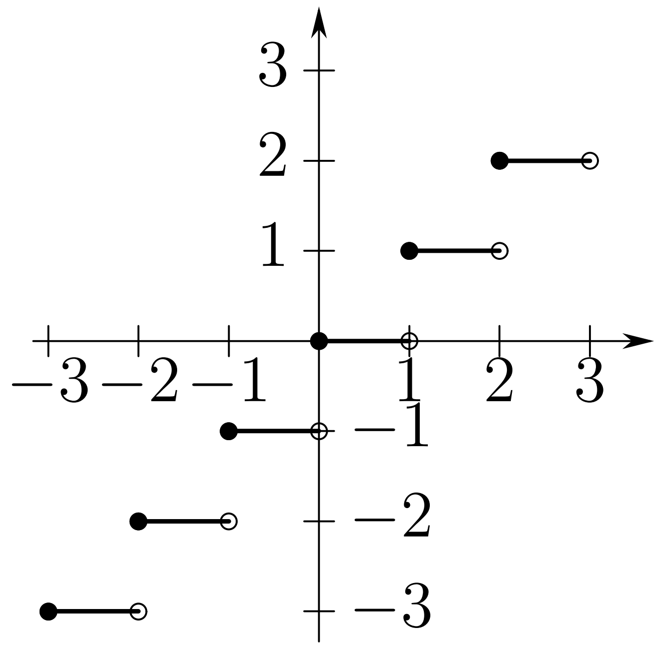


Définition: fonction plancher R(N)

La **fonction plancher** attribue à un nombre réel x le nombre entier le plus grand qui est plus petit que x ou égal à celui-ci. La valeur de la fonction plancher de x est symbolisée par $\lfloor x \rfloor$. La fonction plancher de x est aussi appelée **partie entière** de x.

ex : 2,3 = 2

ex : -3,5 = -4

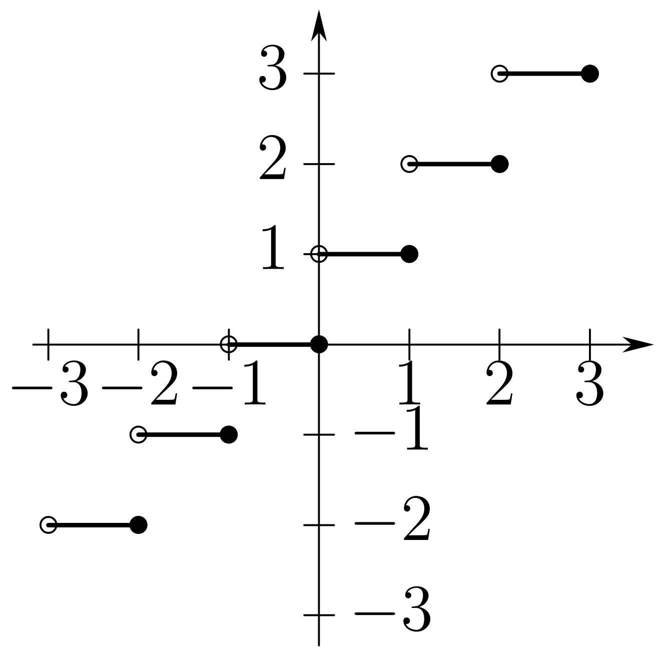


Définition: fonction plafond

La **fonction plafond** attribue à un nombre réel x le nombre entier le plus petit qui est plus grand que x ou égal à celui-ci. La valeur de la fonction plafond de x est symbolisée par $\lceil x \rceil$.

ex: 2,3 = 3

ex: -3,5 = -3



Définition: suite

Une **suite** est une fonction définie sur un sous-ensemble de l'ensemble des entiers (habituellement l'ensemble $\{0, 1, 2, ...\}$ ou l'ensemble $\{1, 2, 3, ...\}$) dans l'ensemble S. On utilisera la notation a_n pour représenter l'image du nombre entier n. On appelle a_n un élément de la suite. On utilise la notation $\{a_n\}$ pour désigner une suite, ce qui est en contradiction avec la notation d'un ensemble.

Définition: somme

La notation servant à exprimer la **somme des éléments de la suite** $\{a_n\}$ est

$$\sum_{j=m}^{n} a_j$$

qui signifie

$$a_m + a_{m+1} + \ldots + a_n.$$

Ici, la variable j est appelée l'**indice de la sommation**.

Définition: produit

La notation servant à exprimer la **produit des éléments de la suite** $\{a_n\}$ est

$$\prod_{j=m}^{n} a_j$$

qui signifie

$$a_m \times a_{m+1} \times \ldots \times a_n.$$

Ici, la variable j est appelée l'**indice du produit**.

Définition: progression géométrique

— Suite géométrique

Une **progression géométrique** est une suite de la forme

$$a, ar, ar^2, ar^3, \ldots, ar^k,$$

où a (l'**élément initial**) et r (la **raison**) sont des nombres réels.

La somme S des $n+1$ premiers éléments de la progression géométrique est donnée par

$$S = \sum_{j=0}^{n} ar^j = \begin{cases} a(n+1) & \textbf{si } r = 1 \\ a\dfrac{r^{n+1}-1}{r-1} & \textbf{si } r \neq 1. \end{cases}$$

La croissance des fonctions

Pour l'étude de la complexité des algorithmes, on veut quantifier le concept qui dit que g *croît au moins aussi vite* que f.

Qu'est-ce qui importe vraiment quand on compare la complexité des algorithmes?

- On se soucie seulement du comportement des algorithmes pour de *grandes instances* du problème.
- Même les mauvais algorithmes peuvent être utilisés pour résoudre les petits cas.
- Dans l'étude du coût des algorithmes, on peut ignorer les détails d'implémentation tels que l'implémentation du compteur de la boucle, etc.

Définition: complexité d'un algorithme

Définition: Soit un algorithme $\mathcal{A}$ et $l(d)$ un entier mesurant la complexité d'une donnée d (sa taille par exemple).

1. On appelle *complexité temporelle* de $\mathcal{A}$ une fonction $ct(\mathcal{A} : \mathbb{N} \rightarrow \mathbb{N})$ telle que si d est une donnée alors $ct(\mathcal{A})(l(d))$ est un majorant du nombre d'opérations élémentaires nécessaires pour obtenir le résultat associé à la donnée d.
2. On appelle *complexité spatiale* de $\mathcal{A}$ une fonction $cs(\mathcal{A} : \mathbb{N} \rightarrow \mathbb{N})$ telle que si d est une donnée alors $cs(\mathcal{A})(l(d))$ est un majorant du nombre d'espaces mémoires nécessaires pour obtenir le résultat associé à la donnée d.

La complexité temporelle est la plus couramment utilisée pour évaluer ou comparer des algorithmes.

Exemples de complexités (1)

- Complexité infra-linéaire : calcul du PGCD ($log_p(n)$, où p est le nombre d'or[a])
- Complexité linéaire : calcul de la valeur d'un pôlynome par le schéma de Horner.
- Complexité polynomiale :
  - Algorithmes de tri (n^2 pour les algos simples, $nlog(n)$ pour des algos plus performants, ...)
  - produit de matrices (n^3) pour l'algo standard, ($n^{2.7}$) pour un algo plus sophistiqué.

[a] racine de l'quation $x^2 = x + 1$ c--d $\frac{1+\sqrt{5}}{2}$

Exemples de complexités (2)

Complexités d'Algorithmes non efficaces:

- Complexité exponentielle : Voyageur de commerce, algorithmes récursifs,
- autres classes de complexité : NP-complets (problèmes mutuellement réductibles les uns aux autres mais ayant une solution exponentielle),

Définition: comportement asymptotique

Nous présentons dans ce qui suit des concepts utiles pour le calcul de la complexité.

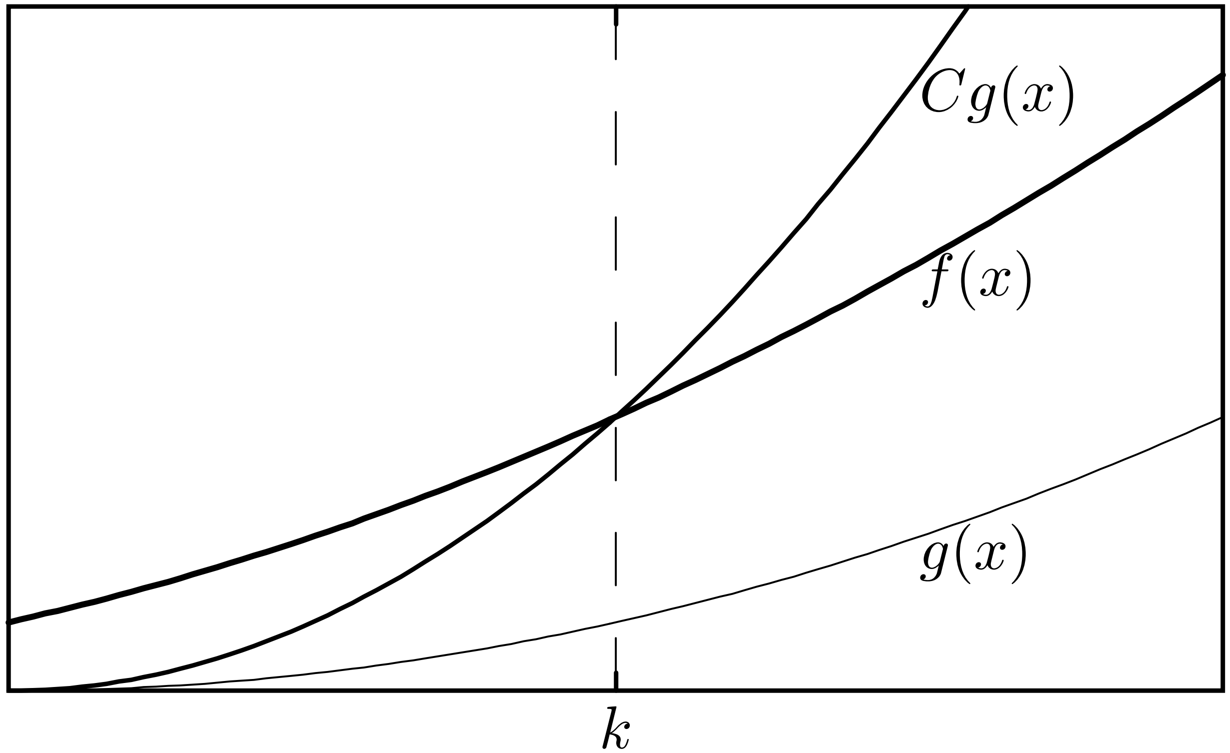
Soit f et g des fonctions de l'ensemble des nombres entiers ou de l'ensemble des nombres réels dans l'ensemble des nombres réels. On dit que $f(x)$ est en $O(g(x))$ s'il existe des constantes C et k telles que

$$\boxed{|f(x)| \leq C|g(x)|}$$

dès que $x > k$. Cette notation se lit $f(x)$ est "**grand** O" de $g(x)$.

$f \in O(g)$ // f est un grand O de g

Comportement asymptotique



Pour tout $x > k$, $f(x) < Cg(x)$ implique que $f(x)$ est $O(g(x))$.

Choix de C et k

Note: Pour démontrer que $f(x)$ est $O(g(x))$, il suffit de prouver qu'une paire de constantes C et k vérifient l'inéquation $|f(x)| \leq C|g(x)|$ si $x > k$. Cependant, cette paire C, k, qui satisfait la définition, n'est jamais unique. Si une telle paire existe, il en existe une infinité d'autres.

Exemple de comportement asymptotique

Soit $f(x) = 7x^2$ et $g(x) = x^3$. Démontrez que $f(x)$ est $O(g(x))$.

L'inégalité $7x^2 < x^3$ est valide dès que $x > 7$. Donc, en prenant $k = 7$ et $C = 1$, on a que

$$|f(x)| \leq C|g(x)|$$

pour tout $x > k$. D'où

$$f(x) \text{ est } O(g(x)).$$

Remarquer que la conclusion est la même pour $C = 2$ et $k = 8$, pour $C = 3.7$ et $k = 12.111$, etc.

Exemple de comportement asymptotique

Soit $f(x) = 7x^2$ et $g(x) = x^2$. Démontrez que $f(x)$ est $O(g(x))$.

En prenant $C = 7$, on a l'égalité $7x^2 = Cx^2$ est valide pour toute valeur de x. Donc,

$$|f(x)| \leq C|g(x)|$$

pour $C = 7$ et pour tout $x > 0$, par exemple. D'où

$$7x^2 \text{ est } O(x^2).$$

Comportement asymptotique des polynômes

Soit

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

où a_0, a_1, ..., a_{n-1} et a_n sont des nombres réels.
Alors

$$f(x) \text{ est } O(x^n).$$

Comportement asymptotique de la factorielle

On a que

$$\begin{aligned} \boxed{n!} &= 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n \\ &\le n \cdot n \cdot n \cdot \cdots \cdot n \\ &= \boxed{n^n.} \end{aligned}$$

Donc $n!$ est $O(n^n)$.

En prenant le logarithme de chaque côté,

$$\log n! \le \log(n^n) = n \log n.$$

Donc $\log n!$ est $O(n \log n)$.

Autres Comportements asymptotiques

Logarithme: On a que $n < 2^n$.. En prenant le logarithme en base 2 de chaque côté, on obtient que $\log_2 n$ est $O(n)$.

Multiplication par un scalaire: Si $f(x)$ est $O(g(x))$, et si a est un nombre réel, alors $af(x)$ est aussi $O(g(x))$.

Addition de deux fonctions de même complexité : Si $f_1(x)$ et $f_2(x)$ sont $O(g(x))$,
alors $f_1(x) + f_x(x)$ est aussi $O(g(x))$.

Transitivité de O

Si

$$f(x) \text{ est } O(g(x)),$$

et si

$$g(x) \text{ est } O(h(x)),$$

alors

$$f(x) \text{ est } O(h(x)).$$

Comportement asymptotique du produit et de l'addition

Si $f_1(x)$ est $O(g_1(x))$,
et si $f_2(x)$ est $O(g_2(x))$,

Produit de deux fonctions :

$$(f_1 f_2)(x) \text{ est } O(g_1(x)\, g_2(x)).$$

Addition de deux fonctions :

$$(f_1 + f_2)(x) \text{ est } O\left(\max(g_1(x), g_2(x))\right).$$

Question: Qu'est-ce que $\max(n \log n, n^2)$ par exemple?

Définition: grand Θ

$f(x)$ est $O(g(x))$ signifie que $g(x)$ *croît au moins aussi vite, sinon plus* que $f(x)$.

$g(x)$ est $O(f(x))$ signifie que $f(x)$ *croît au moins aussi vite, sinon plus* que $g(x)$.

$f(x)$ est $\Theta(g(x))$ signifie que $g(x)$ *croît à la même vitesse* que $f(x)$. On a que $f(x)$ est $\Theta(g(x))$ si et seulement si $f(x)$ est $O(g(x))$ et $g(x)$ est $O(f(x))$.

Aussi, $f(x)$ est $\Theta(g(x))$ implique que $g(x)$ est $\Theta(f(x))$

Définition: grand Θ

Plus formellement, soit $f(x)$ et $g(x)$ des fonctions de l'ensemble des nombres réels ou de l'ensemble des entiers positifs dans l'ensemble des nombres réels. On écrit $f(x)$ est $\Theta(g(x))$ quand il existe des nombres réels positifs C_1 et C_2 et un entier k qui vérifient

$$C_1|g(x)| \leq |f(x)| \leq C_2|g(x)|$$

pour tout $x > k$.

EXEMPLE: $f(x) = 5.5x^2 - 7x$ est en $\Theta(x^2)$.
Il suffit de montrer que ça marche avec
$C_1 = 9, C_2 = 3$ et $k = 2.8$, par exemple.

Classement de la complexité

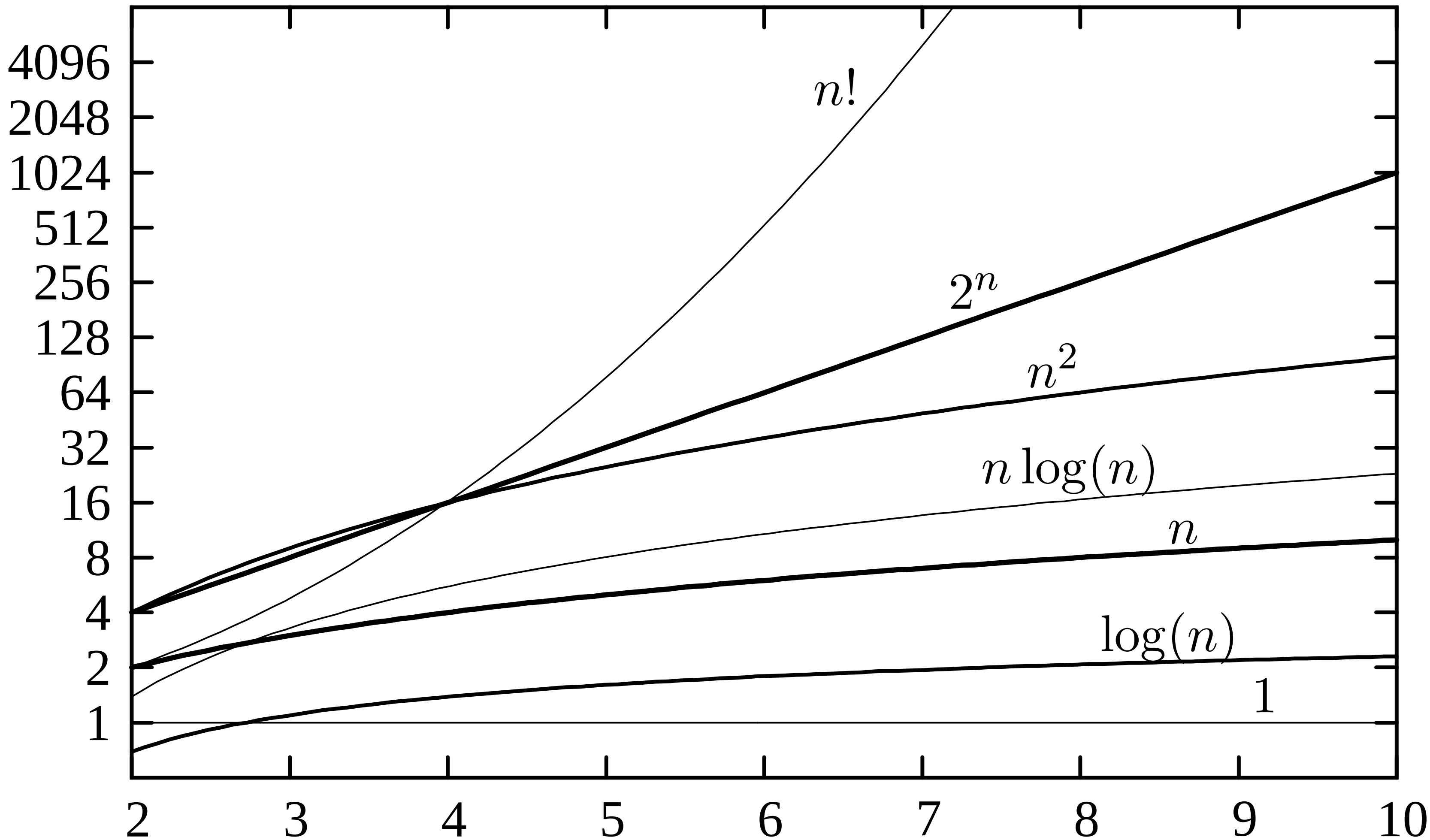
Les différentes classes de complexité s'ordonnent comme suit:

$$O(1) \subseteq O(\log n) \subseteq O(n) \subseteq O(n \log n) \subseteq O(n^2)$$

$$\subseteq O(n^i) \subseteq O(c^n) \subseteq O(n!)$$

pour $i > 2$ et $c > 1$.

Classement de la complexité



Raisonnement mathématique : induction

Induction mathématique

Module Ensembles bien ordonnés (197)

Module Induction mathématique (198)

Module Principe généralisé d'induction (202)

Définition: ensemble bien ordonné

Un ensemble totalement ordonné (S, R) est **bien ordonné** si et seulement si tout sous-ensemble de S a un plus petit élément.

Exemples:

- $(\mathbb{N}, \leq)$ est bien ordonné alors que $(\mathbb{N}, \geq)$ ne l'est pas.
- $([0,1], \leq)$ n'est pas bien ordonné parce que $]0,1] \subset [0,1]$ n'a pas de plus petit élément.
- $(\mathbb{Z}, \leq)$ n'est pas bien ordonné parce que $\mathbb{Z}$ n'a pas de plus petit élément.
- L'ensemble des chaînes finies de caractères alphabétiques avec l'ordre lexicographique est bien ordonné.

Induction mathématique: Énoncé du problème

Définition : Soit $P(n)$, un prédicat sur un ensemble bien ordonné S. Le problème est de prouver que

$$\forall n \in S, P(n)$$

est vraie.

Définition: induction mathématique

Soit $P(n)$, un prédicat sur un ensemble bien ordonné S. Soit 0, l'élément minimal de l'ensemble S. Alors la règle d'inférence

Considérés comme vraies

$$\frac{P(0) \quad \forall n(P(n) \rightarrow P(n+1))}{\forall n\, P(n)}$$

Hyp

} Conclusion

est connue sous le nom de **principe de l'induction** (ou **premier principe de l'induction**).

La première hypothèse $P(0)$ est appelée **étape de base**.

La deuxième hypothèse $P(n) \rightarrow P(n+1)$ pour un n quelconque, est appelée **étape inductive**.

Exemple: la somme des n premiers entiers

Soit $P(n)$, la fonction propositionnelle “la somme des n premiers entiers positifs est $n(n+1)/2$”.

1 Étape de base: On doit démontrer que $P(1)$ est vrai.

2 Étape inductive: On doit démontrer que $P(n) \rightarrow P(n+1)$ pour tout entier positif n.

3 On conclut que $P(n)$ est vraie pour tout entier positif n.

Fondements de l'induction mathématique

Supposons que S est $\mathbb{N}$, que $P(0)$ est vrai et que la proposition $P(n) \rightarrow P(n+1)$ est vrai pour un n quelconque. Pour démontrer que $P(n)$ doit est vraie pour tout $n \in \mathbb{N}$, on utilise une preuve par l'absurde.
On suppose qu'il existe au moins un entier positif pour lequel $P(n)$ est fausse. Alors, l'ensemble $T \subset \mathbb{N}$ pour lequel $P(n)$ est fausse est non vide. Ainsi, selon le principe du bon ordre, T comprend un plus petit élément, lequel sera désigné par k. On sait que k ne peut être 0 car $P(0)$ est vraie.
Donc k est un entier plus grand que 0 et $k-1 \in \mathbb{N}$. De plus, $k-1$ est inférieur à k et n'appartient pas à T, donc $P(k-1)$ doit être vraie.
Puisque l'implication $P(n) \rightarrow P(n+1)$ est vraie pour un n quelconque, on a que $P(k-1) \rightarrow P(k)$ et donc $P(k)$ est vraie.
Ce qui contredit le choix de k.

Définition: principe généralisé d'induction

Soit $P(n)$, un prédicat sur un ensemble bien ordonné S. Alors la règle d'inférence

$$\frac{P(0) \quad \forall n[(P(1) \land P(2) \land \ldots \land P(n)) \to P(n+1)]}{\forall n\, P(n)}$$

est connue sous le nom de **principe généralisé de l'induction** (ou **deuxième principe de l'induction**).

Quand on hésite sur le choix d'une induction il est préférable d'utiliser le principe généralisé.
Cependant, il existe d'autre méthodes pour l'induction (voir notamment 209).

Exemple du principe généralisé d'induction

Soit $S = \mathbb{N} - \{0, 1\}$. Soit $P(n)$ la proposition "n peut s'écrire comme le produit de nombres premiers".

Étape de base: On doit démontrer que $P(2)$ est vrai.

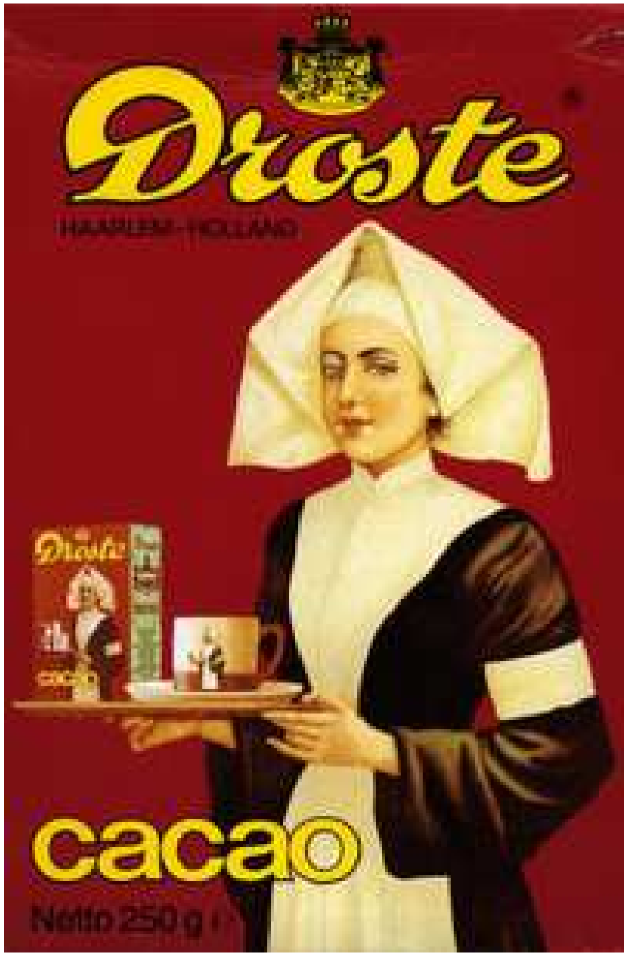
Étape inductive: On suppose que $P(k)$ est vraie pour tout entier positif k avec $k \leq n$. Il faut démontrer que $P(n+1)$ est vraie selon cette hypothèse:
- ou bien $n + 1$ est premier alors il possède un diviseur premier qui est lui-même,
- ou bien $n + 1$ est composé et il existe deux entiers d et d' compris entre 2 et n tels que $n + 1 = dd'$. Alors d et d' possèdent des diviseurs premiers qui sont aussi diviseurs de $n + 1$.

On conclut que $P(n)$ est vraie pour tout entier positif n.

Module Récursivité et Itération

Récursivité et itération

Récursivité et itération



www.droste.nl

Définition: fonction récursive

Pour définir une fonction qui a l'ensemble des entiers non négatifs pour domaine, on procède de la manière suivante:

ÉTAPE DE BASE: On précise la valeur de la fonction en zéro.

ÉTAPE INDUCTIVE: On donne la règle pour trouver la valeur de la fonction pour de nouveaux entiers à partir de la valeur de la fonction pour des entiers plus petits.

Cette définition d'une fonction est dite **récursive** ou **inductive**.

Quelques définitions inductives

a^n :
ÉTAPE DE BASE: $f(0) = a^0 = 1$
ÉTAPE INDUCTIVE: $f(n+1) = a^{n+1} = a \cdot f(n)$ pour $n \geq 1$.

Factorielle :
ÉTAPE DE BASE: $F(0) = 1$ factorielle de 0 est tjs 1
ÉTAPE INDUCTIVE: $F(n+1) = (n+1)F(n)$ pour $n \geq 1$.

Suite de Fibonacci:
ÉTAPE DE BASE: $f_0 = 0$ et $f_1 = 1$.
ÉTAPE INDUCTIVE: $f_{n+1} = f_n + f_{n-1}$ pour $n \geq 2$.

Note historique: Léonard de Pise

Leonardo Pisano, mieux connu sous le nom de **Fibonacci**.
Né en 1170 probablement à Pise.
Mort en 1250 probablement à Pise.

`www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Fibonacci.html`

Définition: Induction structurelle

L'*induction structurelle* permet de vérifier des propriétés sur des structures définies de façon inductive.

Principe de l'induction structurelle : Etant donné un type d'objet défini récursivement , soit P une propriété pouvant porter sur ce type d'objet, si P est vraie pour tout objet de base et si P est conservée à chaque pas de la construction d'un objet de ce type, alors: P est vraie pour tout objet de ce type.

Nous présentons ci-après des exemples de constructions inductives

Ensemble défini récursivement

Pour définir un ensemble récursivement

ÉTAPE DE BASE: Un ensemble initial d'éléments est donné.

ÉTAPE INDUCTIVE: Les règles pour former les éléments de l'ensemble à partir d'autres éléments déjà connus sont données.

Définitions récursives

Nombres naturels :

- ÉTAPE DE BASE: 0 est dans $\mathbb{N}$.
- ÉTAPE INDUCTIVE: Si n est dans $\mathbb{N}$, alors $n + 1$ aussi.

Entiers divisible par trois :

- ÉTAPE DE BASE: 3 appartient à S.
- ÉTAPE INDUCTIVE: Si x et y appartiennent à S, alors $x + y$

appartient à S.

" si X élément de S, alors X+3 est élément de S

Définition: mot d'un alphabet

Un **mot** (**chaîne**) d'un alphabet Σ est une suite finie de symboles de Σ.

L'**ensemble des mots** de Σ est notée Σ^*.

Concaténation de 2 mots: si $x = abra$ et $y = cadabra$, alors $x.y$ donne $abracadabra$.

Σ^* se définit récursivement:

- ÉTAPE DE BASE: ϵ appartient à Σ^* où ϵ est le mot vide.
- ÉTAPE INDUCTIVE: si w appartient à Σ^* et x appartient à Σ, alors wx appartient à Σ^*.

NOTES:

Les mots de longueur infinie ne peuvent pas être dans Σ^*.

On peut définir récursivement la longueur d'un mot.

Formules bien formées

L'induction structurelle est couramment utilisée pour définir des **formules bien formées** dans différents systèmes.

Exemples :

- ensemble des mots de parenthèses bien formées,
- l'ensemble des propositions composées bien formées.

Définition: ensemble des mots de parenthèses bien formées

Définition récursive de l'ensemble P des **mots de parenthèses bien formées**.

ÉTAPE DE BASE: $()$ appartient à P.

ÉTAPE INDUCTIVE: Si w appartient à P, alors $()w$, (w) et $w()$ appartiennent à P.

EXEMPLES:
$(()())$ appartient à P.
$))(()$ n'appartient pas à P.

Définition: ensemble des propositions composées bien formées

Définition récursive de l'ensemble des **propositions composées bien formées** comprenant V, F, des variables propositionnelles et les opérateurs $\{\neg, \vee, \wedge, \rightarrow, \leftrightarrow\}$.

ÉTAPE DE BASE: V, F et p, où p est une variable propositionnelle, sont des propositions composées bien formées.

ÉTAPE INDUCTIVE: Si p et q sont des propositions composées bien formées, alors $(\neg p)$, $(p \vee q)$, $(p \wedge q)$, $(p \rightarrow q)$ et $(p \leftrightarrow q)$ le sont aussi.

EXEMPLES:
$((p \vee q) \rightarrow (r \wedge \mathrm{V}))$ est bien formée.
$\rightarrow(\neg \ \wedge q)\leftrightarrow$ n'est pas bien formée.

Définition: algorithme récursif

Un algorithme est dit **récursif** s'il permet de résoudre un problème en le réduisant au même problème avec une entrée de plus petite taille.

Le principe de base :

1. Une ou plusieurs conditions d'arrêt, pour traiter les cas de base,
2. Un ou plusieurs appels récursifs, qui permettent de résoudre le problème à traiter à partir d'appels sur des arguments plus petits.

Pour que l'algorithme termine, il faut veiller à ce que la suite des appels récursifs conduise toujours à un cas de base, géré par une condition d'arrêt.

Algorithme récursif pour calculer a^n

ÉTAPE DE BASE: $f(0) = a^0 = 1$

ÉTAPE INDUCTIVE: $f(n+1) = a^{n+1} = a \cdot f(n)$ pour $n \geq 1$.

procédure *puissance*
    (a: nombre réel non nul, n: entier positif ou nul)
si $n = 0$ **alors** *puissance*$(a, n) := 1$
sinon *puissance*$(a, n) := a *$ *puissance*$(a, n-1)$

étape de base

est dans 1

Puissance(a, n+1) := a * puissance(a, n)

Concaténation c'est pour former des mots

Algorithme récursif pour la factorielle

ÉTAPE DE BASE: $F(1) = 1$

ÉTAPE INDUCTIVE: $F(n+1) = (n+1)F(n)$ pour $n \geq 2$.

procédure *factorielle* (n: entier positif)
si $n = 1$ **alors**
  factorielle$(n) := 1$
sinon
  factorielle$(n) := n * $ *factorielle*$(n-1)$

factorielle $(n+1) := (n+1) *$ factorielle(n)

Algorithme récursif et pile

Les algorithmes récursifs utilisent une pile.

Une pile est une structure de données dont les entrées peuvent être ajoutées (empilées) et enlevées (dépilées) seulement à partir du dessus.

Dans un algorithme récursif, l'opération courante est suspendue et ses paramètres sont empilés.

Algorithme récursif pour les nombres de Fibonacci

ÉTAPE DE BASE: $f_0 = 0$ et $f_1 = 1$.

ÉTAPE INDUCTIVE: $f_{n+1} = f_n + f_{n-1}$ pour $n \geq 2$.

procédure *fibonacci* (n: entier non négatif)
si $n = 0$ **alors** *fibonacci*(0) := 0
sinon si $n = 1$ **alors** *fibonacci*(1) := 1
sinon *fibonacci*(n) := *fibonacci*$(n-1)$ + *fibonacci*$(n -$

Algorithme récursif pour la recherche binaire

On veut trouver x dans la suite ordonnée $a_1, a_2, \ldots, a_n$.

procédure *fouille binaire*(x, i, j)
$m := \lfloor (i+j)/2 \rfloor$
si $x = a_m$ **alors**
    emplacement $:= m$
sinon si $(x < a_m$ et $i < m)$ **alors**
    fouille binaire$(x, i, m-1)$
sinon si $(x > a_m$ et $j > m)$ **alors**
    fouille binaire$(x, m+1, j)$
sinon emplacement $:= 0$

Élimination de la Récursivité

- Avantages des algorithmes récursifs :

  Fiabilité : Solution naturelle et facile à concevoir :

  - si la fonction est récursive
  - quand la structure de données traitée est récursive

- Inconvénients :
  - Perte de performances (gestion de la pile coûteuse)
  - Problème d'encombrement mémoire

Comment éliminer la récursivité?

- Écrire un algorithme itératif équivalent
- Gérer dans l'algorithme la pile des sauvegardes => ne garder que celles utiles

Algorithme itératif pour la factorielle

procédure *factorielle itérative* (n: entier positif)
$x := 1$
pour $i := 1$ **à** n
    $x := i * x$
$\{x$ est $n!\}$

Quel est le coût de cet algorithme? Comparer avec l'algoritme récursif.

Algorithme itératif pour les nombres de Fibonacci

procédure *fibonacci itératif* (n: entier non négatif)
si $n = 0$ **alors** $y := 0$
sinon
début
    $x := 0$
    $y := 1$
    pour $i :=$ 1 **à** $n - 1$
    début
        $z := x + y$
        $x := y$
        $y := z$
    fin
fin
$\{y$ est le n-ième nombre de Fibonacci$\}$

Quel est le coût de cet algorithme? Comparer avec l'algoritme récursif.

Fermetures de Relations

Module Fermeture des relations (225)

- Fermeture d'une relation (226)
- Fermeture réflexive (227) • Fermeture symétrique (229)
- Composition de relations (232) • Chemin, longueur et Puissance (233)
- Produit booléen de deux matrices (234)
- Disjonction booléenne de deux matrices (235)
- Propriété des relations transitives (236) • Relation de connexité (237)
- Fermeture transitive (239)
- Algorithme de fermeture transitive (242)

Définition: fermeture d'une relation

Soit R une relation dans un ensemble A. La relation R peut ou non admettre une propriété $\mathbf{P}$ comme la réflexivité, la symétrie ou la transitivité.

S'il existe une relation S

- qui admet la propriété $\mathbf{P}$,
- qui contient R
- et telle que S est un sous-ensemble de chaque relation avec la propriété $\mathbf{P}$ qui contient R,

alors S est appelé la **fermeture** ou **clôture convenable** de R par rapport à $\mathbf{P}$.

Fermeture réflexive

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$.

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Quelle est la fermeture réflexive de R? } le S

(1,1) (2,2) (3,3) (4,4) qui est le Δ

ne se répètent pas car ∪

Définition: fermeture réflexive

Soit R, une relation dans un ensemble A. La fermeture réflexive de R est

$$R \cup \Delta$$

où

$$\Delta = \{(a, a) \mid a \in A\}$$

est appelée la **relation diagonale** dans A.

(a, a)

Fermeture symétrique

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1), (1,2), (2,1), (2,2), (3,4), (4,1), (4,4)\}$.

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

Quelle est la fermeture symétrique de R?

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

Définition: fermeture symétrique

Soit R, une relation dans un ensemble A. La fermeture symétrique de R est

$$R \cup R^{-1}$$

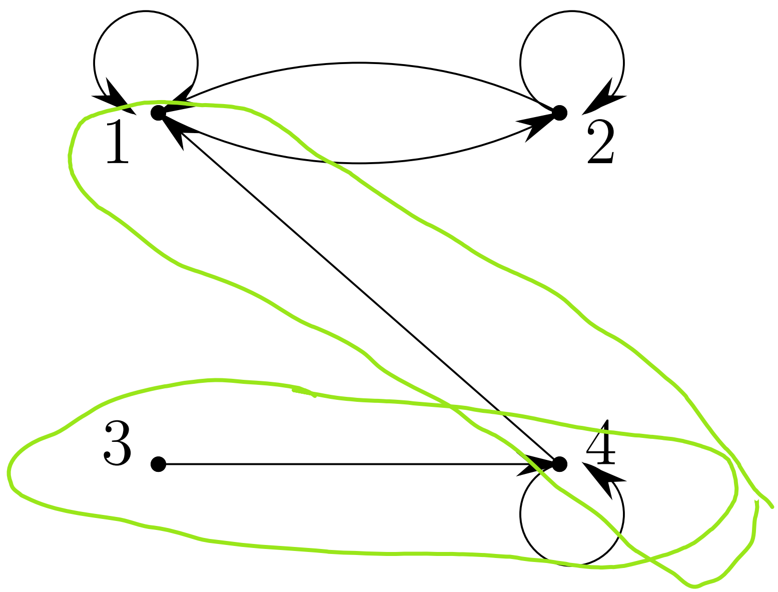
où

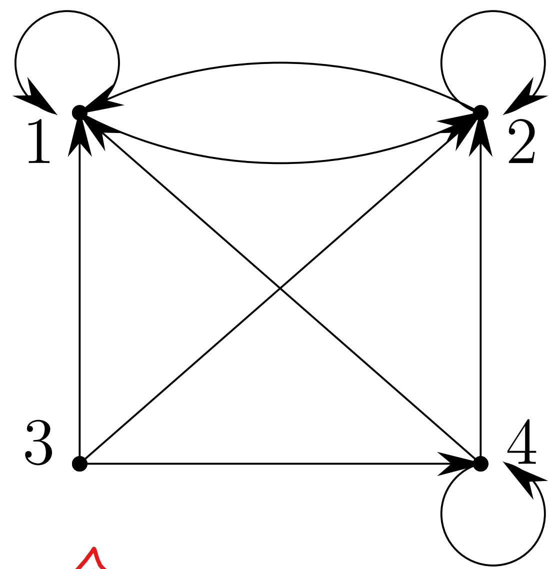
$$R^{-1} = \{(b, a) \mid (a, b) \in R\}$$

est la **relation inverse** de R.

Fermeture transitive

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1),(1,2),(2,1),(2,2),(3,4),(4,1),(4,4)\}$. Quelle est la fermeture transitive de R?



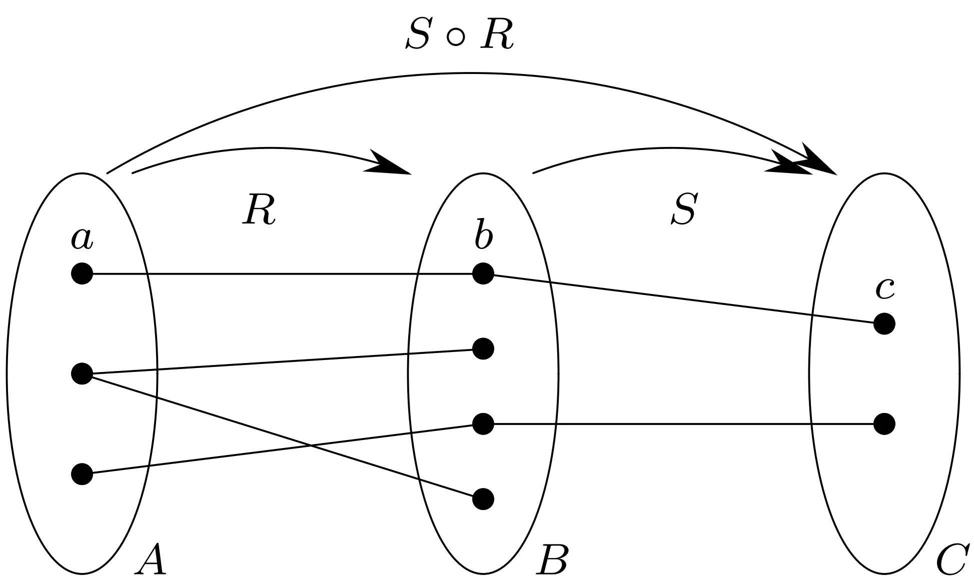


Il manque 3 et 1

ici ajoutée

Définitions: composition de relations

Soit R une relation d'un ensemble A à un ensemble B, et S une relation de B à un ensemble C. La **composition de** R **et** S est la relation constituée des couples (a, c), où $a \in A$, $c \in C$ et pour laquelle il existe un élément $b \in B$ tel que $(a, b) \in R$ et $(b, c) \in S$. On note cette composition de R et S par $S \circ R$.



Définitions: chemin, longueur et puissance

Un **chemin** de a à b dans une relation R s'il y a une suite d'éléments $a, x_1, x_2, ..., x_{n-1}, b$ avec $(a, x_1) \in R$, $(x_1, x_2) \in R$, ..., $(x_{n-1}, b) \in R$. Le chemin est de **longueur** n.

Puissance d'une relation : Soit R une relation dans l'ensemble A. Les **puissances** R^n, $n = 1, 2, ...,$ sont définies récursivement selon

$$R^1 = R \quad \text{et} \quad R^{n+1} = R^n \circ R.$$

Définition: produit booléen de deux matrices

Soit $\mathbf{A} = [a_{ij}]$ une matrice booléenne $m \times k$ et $\mathbf{B} = [b_{ij}]$ une matrice booléenne $k \times n$. Alors, le **produit booléen** de $\mathbf{A}$ par $\mathbf{B}$, symbolisé par $\mathbf{A} \odot \mathbf{B}$, est la matrice $m \times n$ avec comme (i, j)-ième élément $[c_{ij}]$, où

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \ldots \vee (a_{ik} \wedge b_{kj}).$$

Note 1: $\mathbf{M}_{S \circ R} = \mathbf{M}_R \odot \mathbf{M}_S$.

Note 2: $\mathbf{M}_{R \circ R} = \mathbf{M}_R \odot \mathbf{M}_R = \mathbf{M}_R^{[2]}$.

Définition: disjonction booléenne de deux matrices

Soit $\mathbf{A} = [a_{ij}]$ et $\mathbf{B} = [b_{ij}]$ les matrices booléennes $m \times n$. Alors, la **disjonction booléenne** de $\mathbf{A}$ et de $\mathbf{B}$, symbolisée par $\mathbf{A} \vee \mathbf{B}$, est la matrice booléenne $m \times n$ avec comme (i,j)-ième élément $a_{ij} \vee b_{ij}$.

Exemple. Soit

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \quad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Alors

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Propriété des relations transitives

THEORÈME 1 :
Une relation R dans un ensemble A est transitive si et seulement si $R^n \subseteq R$ pour $n > 0$.

Démonstration: R^n sous ensemble de R

- $\Leftarrow$ On suppose que R^n et en particulier R^2 est transitive et on montre facilement que R est transitive: aRb et bRc donc aR^2c, et finalement aRc car R^2 est incluse dans R.
- $\Rightarrow$ on utilise un raisonnement par récurrence sur n.

Définition: relation de connexité

Soit R une relation dans un ensemble A. La **relation de connexité** R^* est constituée des couples (a, b) de telle sorte qu'il existe un chemin entre a et b dans R.

THÉORÈME 2 : La **fermeture transitive d'une relation** R est égale à la relation de connexité R^*.

Démonstration page suivante.

Démonstration

- R^* contient R,
- R^* est transitive: Soient aR^*b et bR^*c. Par définition, il existe un chemin de a vers b et un chemin de b vers c dans R^*; d'où, il existe un chemin de a vers c dans R^* et R^* est transitive.
- Soit S une relation transitive contenant R. S^n est transitive et $S^n \subseteq S$ (Th.1). De plus par définition de S^*, on a $S^* \subseteq S$ ($S^* = S^1 \cup S^2 \cup ... \cup S^k$... et $S^k \subseteq S$). Puisque $R \subseteq S$, on a $R^* \subseteq S^*$ car tout chemin de R est également chemin de S. D'où $R^* \subseteq S^* \subseteq S$. Toute relation transitive contenant R doit contenir R^*. Donc R^* est la fermeture transitive de R.

Définition: fermeture transitive

THÉORÈME 3 : Soit $\mathbf{M}_R$, la matrice booléenne d'une relation R dans un ensemble à n éléments. Alors la matrice booléenne de la fermeture transitive R^* est

$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]} \vee \cdots \vee \mathbf{M}_R^{[n]}$$

Démonstration page suivante. Disjonction

Démonstration (1)

La démonstration utilise le lemme suivant:

LEMME : Soit une relation R dans un ensemble A de cardinal n. S'il existe un chemin dans R de a vers b, alors il existe un chemin de a vers b de longueur inférieure ou égale à n. De plus si $a \neq b$ la longueur du chemin ne dépasse pas $n - 1$.

La démonstration du lemme utilise le principe des nids de pigeons. S'il y a plus de n noeuds dans le chemin alors forcément ce chemin contient deux fois le même sommet disons x_i. Il y a donc un circuit de x_i à lui-même, que l'on enlève. Ainsi le chemin de a vers b est de longueur inférieure ou égale à n.

Démonstration (2)

Le lemme 1 indique que :

$$R^* = R_1 \cup R^2 \cup \ldots \cup R^n.$$

En effet, il y a un chemin dans R^* entre 2 sommets, ssi il y a un chemin entre ces sommets dans R^i pour un certain $i \leq n$.
Or la matrice booléenne d'une union de relations est la disjonction des matrices booléennes de ces relations. On en déduit que la matrice booléenne de la fermeture transitive est la disjonction des matrices booléennes des n premières puissances de la matrice booléenne de R.

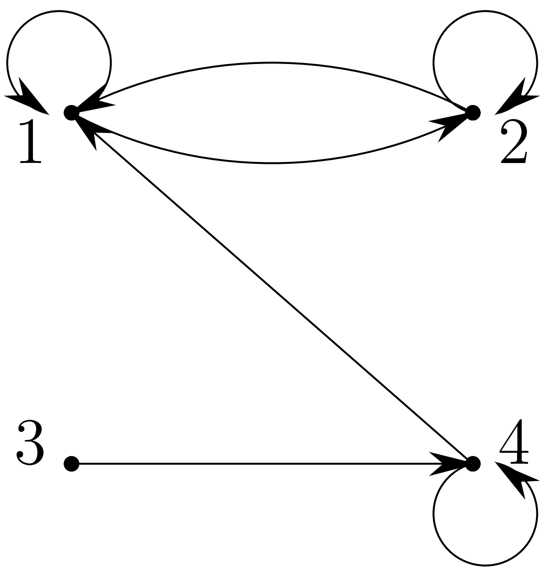
De ce théorème on déduit l'algorithme suivant de calcul de la fermeture transitive:

Algorithme de fermeture transitive

procédure *fermeture transitive*
($\mathbf{M}_R$: matrice booléenne $n \times n$)
$\mathbf{A} := \mathbf{M}_R$
$\mathbf{B} := \mathbf{A}$
pour $i := 2$ **à** n
début
$\mathbf{A} := \mathbf{A} \odot \mathbf{M}_R$
$\mathbf{B} := \mathbf{B} \vee \mathbf{A}$
fin $\{B$ est la matrice booléenne de $R^*\}$

Exemple de fermeture transitive, étape 1 de 4

Soit A l'ensemble $\{1, 2, 3, 4\}$. Soit la relation $R = \{(1,1),(1,2),(2,1),(2,2),(3,4),(4,1),(4,4)\}$. Quelle est la fermeture transitive de R?



$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

Exemple de fermeture transitive, étape 2 de 4

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{M}_R^{[2]} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

$$\mathbf{M}_R^{[3]} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \qquad \mathbf{M}_R^{[4]} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

change plus, identiques

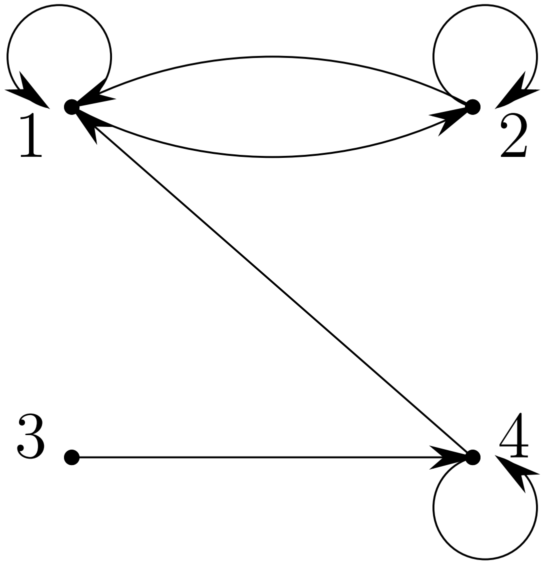
Exemple de fermeture transitive, étape 3 de 4

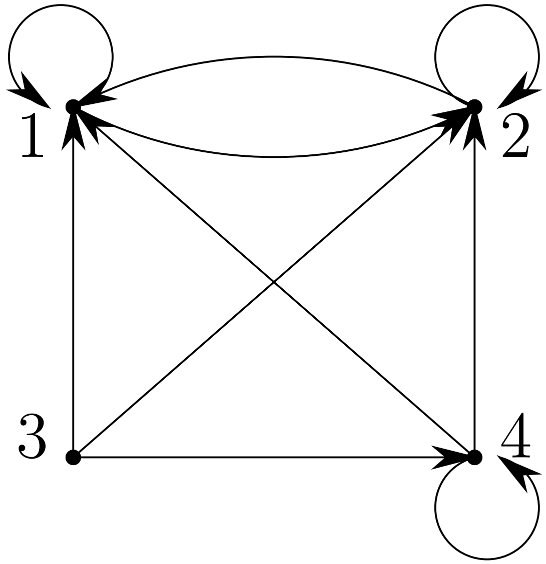
$$\mathbf{M}_{R^*} = \mathbf{M}_R \vee \mathbf{M}_R^{[2]} \vee \mathbf{M}_R^{[3]} \vee \mathbf{M}_R^{[4]}$$

$$\mathbf{M}_{R^*} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

Exemple de fermeture transi-tive, étape 4 de 4

$$\mathbf{M}_R = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \qquad \mathbf{M}_{R^*} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$





Module Ordre

Ordres

Définition: ordre lexicographique

Soit deux ensembles partiellement ordonnés $(S_1, \preccurlyeq_1)$ et $(S_2, \preccurlyeq_2)$. L'**ordre de classement** ou **ordre lexicographique strict** $\prec$ sur le produit cartésien $S_1 \times S_2$ est donné par

$$(a_1, a_2) \prec (b_1, b_2) \quad \text{si et seulement si}$$

$$a_1 \prec_1 b_1$$

ou

$$a_1 = b_1 \text{ et } a_2 \prec_2 b_2.$$

Exemple d'ordre lexicographique

Soit S_1, l'alphabet et $\preccurlyeq_1$ l'ordre alphabétique. Soit S_2, l'ensemble $\{0, 1, 2, 3, ..., 9\}$ et $\preccurlyeq_2$ la relation d'ordre $\leq$ habituelle. Alors

- $(A, 7) \prec (B, 1)$ parce que $A \prec_1 B$.
- $(C, 4) \prec (C, 7)$ parce que $C = C$ et $4 \prec_2 7$.

Définition: ordre lexicographique (n-uplets)

On peut définir un un ordre lexicographique du produit cartésien de n ensembles partiellement ordonnés $(S_1, \preccurlyeq_1)$, $(S_2, \preccurlyeq_2)$, ..., $(S_n, \preccurlyeq_n)$. On définit la relation de préordre $\prec$ de $A_1 \times A_2 \times \cdots \times A_n$ par

$$(a_1, a_2, ..., a_n) \prec (b_1, b_2, ..., b_n)$$

si $a_1 \prec_1 b_1$ ou s'il y a un entier $i > 0$ tel que $a_1 = b_1$, ..., $a_i = b_i$ et $a_{i+1} \prec_{i+1} b_{i+1}$.

Exemple d'ordre lexicographique

Soit S_1, l'alphabet et $\preccurlyeq_1$ l'ordre alphabétique. Soit S_2, l'ensemble $\{0, 1, 2, 3, ..., 9\}$ et $\preccurlyeq_2$ la relation d'ordre $\leq$ habituelle. Alors, pour les codes postaux,

- $(G, 9, X, 8, W, 7) \prec (H, 1, A, 2, B, 1)$ parce que $G \prec_1 H$.
- $(G, 1, K, 2, P, 4) \prec (G, 1, K, 7, A, 1)$ parce que $G = G$, $1 = 1$, $K = K$, $2 \prec_2 7$.

Définition: ordre lexicographique (chaînes)

On considère les chaînes $a_1a_2\cdots a_m$ et $b_1b_2\cdots b_n$ dans un ensemble partiellement ordonné S. On suppose que ces chaînes ne sont pas égales. Soit t la valeur minimale de m et n. Selon la définition d'un ordre de classement, la chaîne $a_1a_2\cdots a_m$ est plus petite que la chaîne $b_1b_2\cdots b_n$ si et seulement si

$$(a_1, a_2, .., a_t) \prec (b_1, b_2, ..., b_t)$$

ou

$$(a_1, a_2, .., a_t) = (b_1, b_2, ..., b_t)$$

et $m < n$, où $\prec$ dans cette inégalité représente l'ordre de classement de S^t.

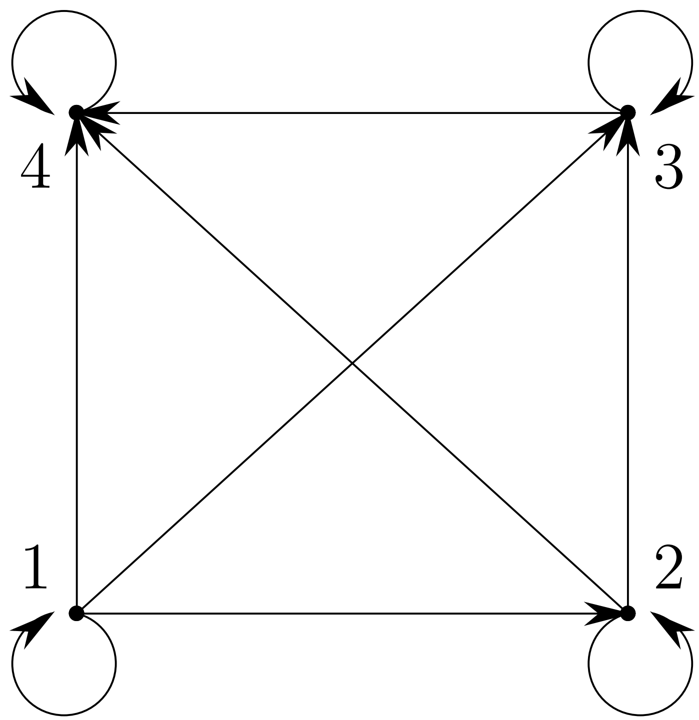
Note historique: Helmut Hasse

Né le 25 août 1898 à Kassel, Allemagne.
Mort le 26 décembre 1979 à Hambourg, Allemagne.

www-groups.dcs.st-and.ac.uk/
˜history/Mathematicians/Hasse.

Exemple $(\{1, 2, 3, 4\}, \leq)$

Soit l'ensemble $S = \{1, 2, 3, 4\}$ et la relation R "$a \leq b$". Cette relation est donnée par $R =$ $\{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (2, 3), (2, 4), (3, 3), (3$

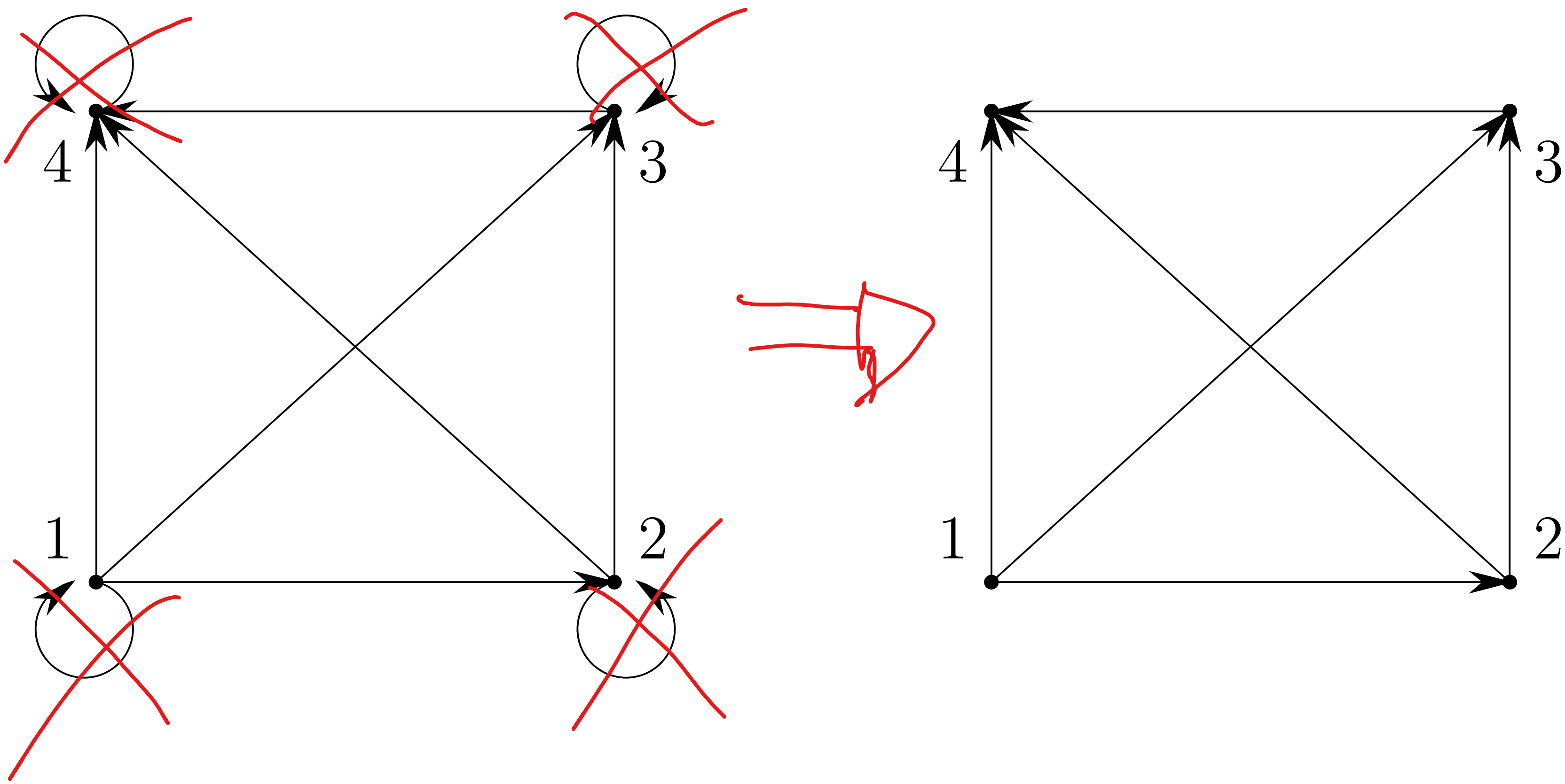


Cette relation est réflexive, antisymétrique et transitive. } Relation d'ordre partiel

Construction du diagramme de Hasse

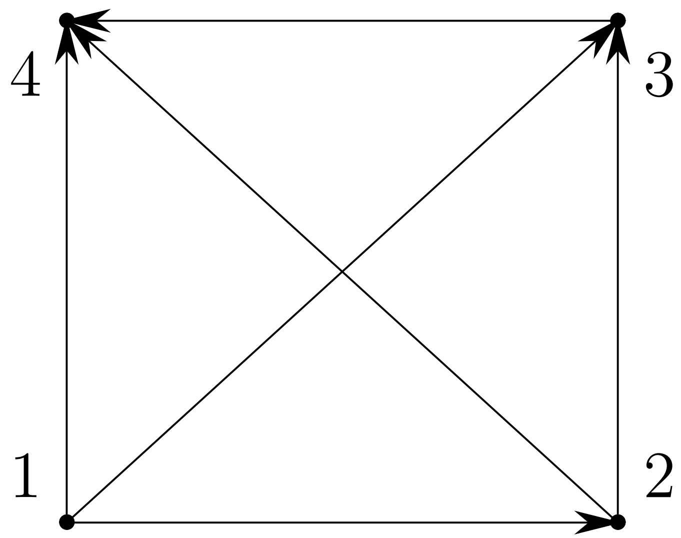
Un diagramme de Hasse est une représentation visuelle d'un ordre fini, qui en facilite la compréhension.

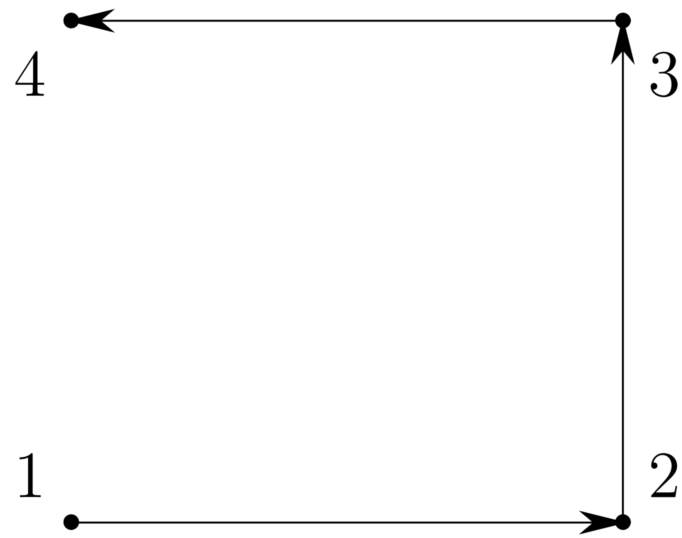
Étape 1 de 4: On enlève les boucles dues à la réflexivité.



Construction du diagramme de Hasse

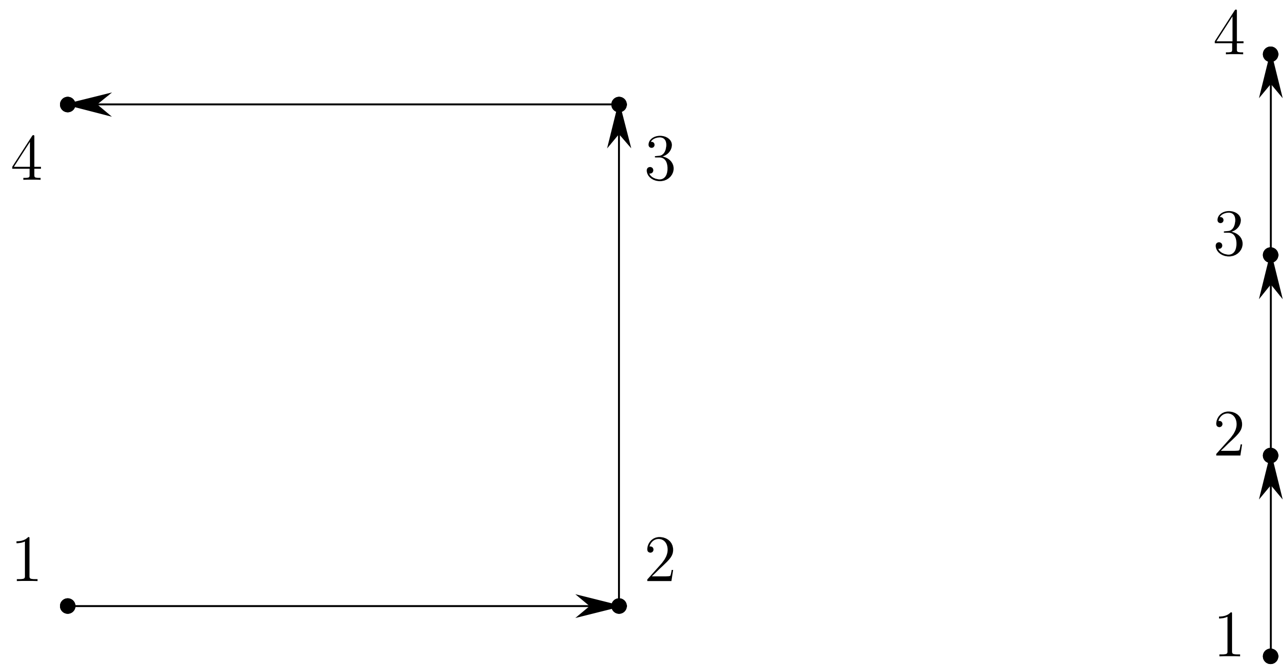
Étape 2 de 4: On enlève les arcs dues à la transitivité.





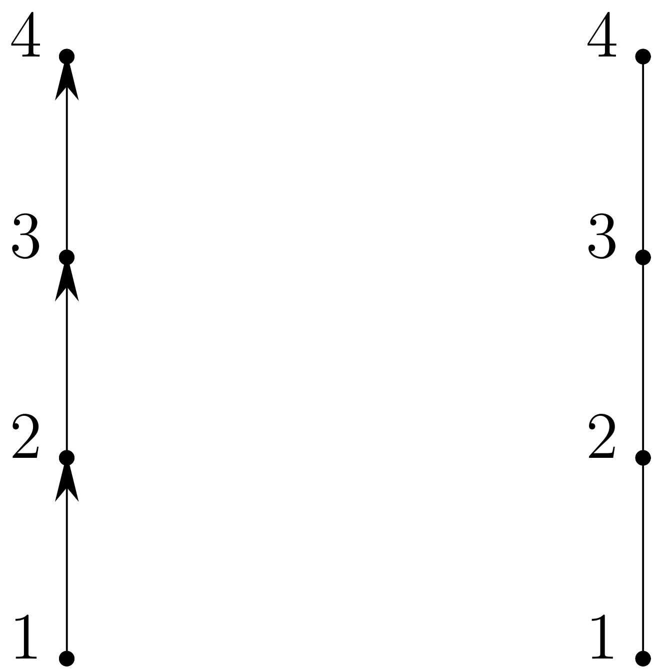
Construction du diagramme de Hasse

Étape 3 de 4: On dispose chaque arc pour que son sommet initial se situe en dessous de son sommet final.



Construction du diagramme de Hasse

Étape 4 de 4: On retire toutes les flèches sur les arcs orientés puisque tous les arcs pointent vers le haut. Le diagramme de droite est le diagramme de Hasse.



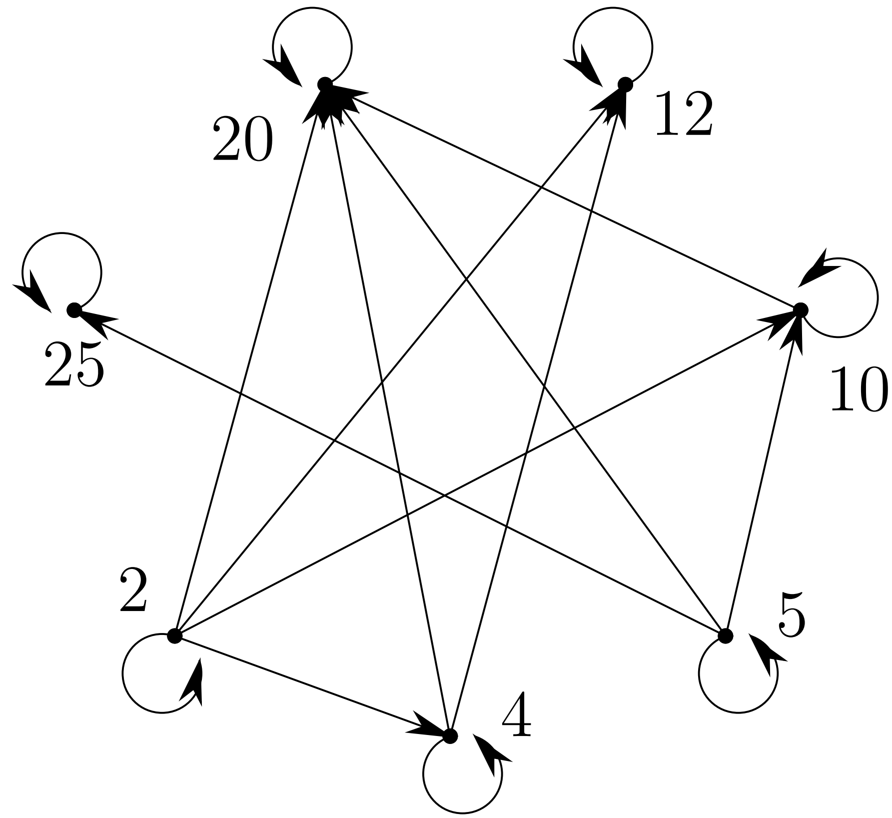
Exemple $(\{2,4,5,10,12,20,25\},|)$

Soit l'ensemble partiellement ordonné $(\{2,4,5,10,12,20,25\},R)$ où R est la relation de préordre $a \mid b$.

$R =$
$\{(2,2),(2,4),(2,10),(2,12),(2,20),(4,4),(4,12),(4,2$
$(5,5),(5,20),(5,25),(10,10),(10,20),(20,20),(25,25$

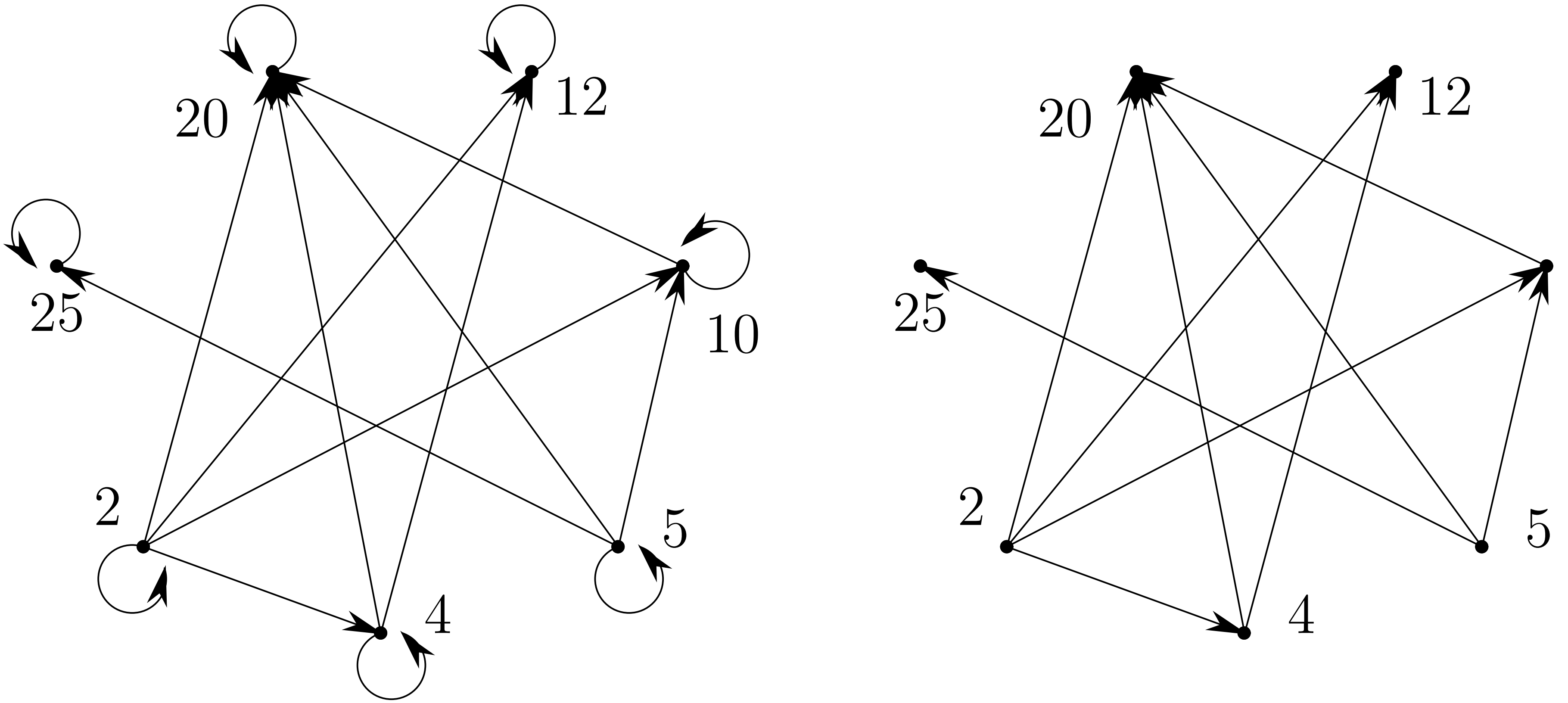
Exemple $(\{2, 4, 5, 10, 12, 20, 25\}, |)$

Cette relation est réflexive, antisymétrique et transitive.



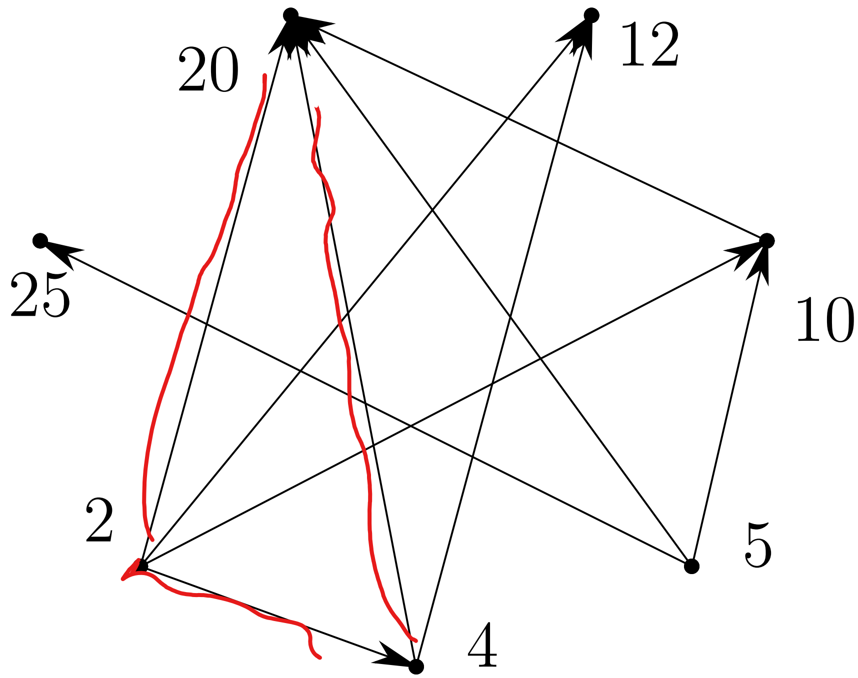
Construction du diagramme de Hasse

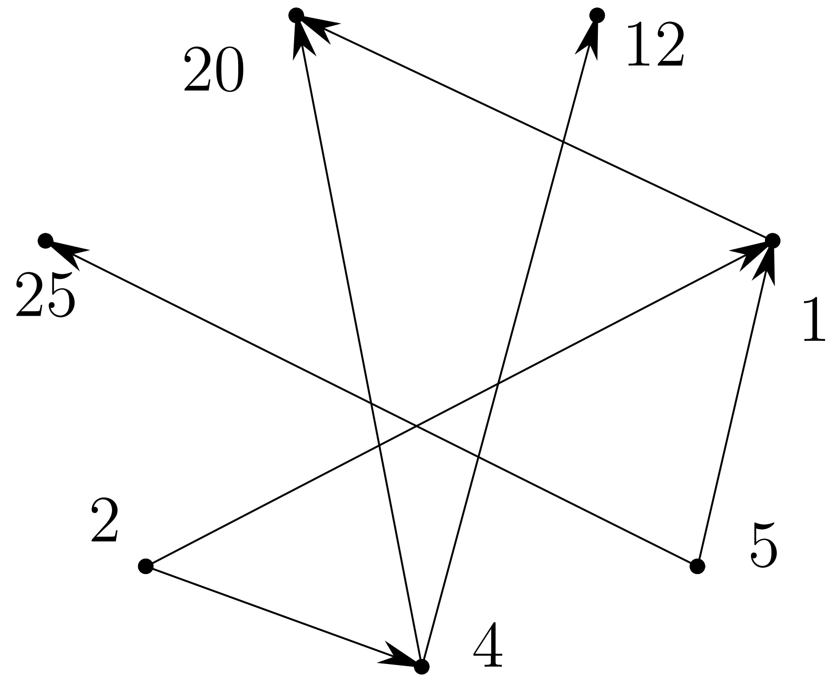
Étape 1 de 4: On enlève les boucles dues à la réflexivité.



Construction du diagramme de Hasse

Étape 2 de 4: On enlève les arcs dues à la transitivité.



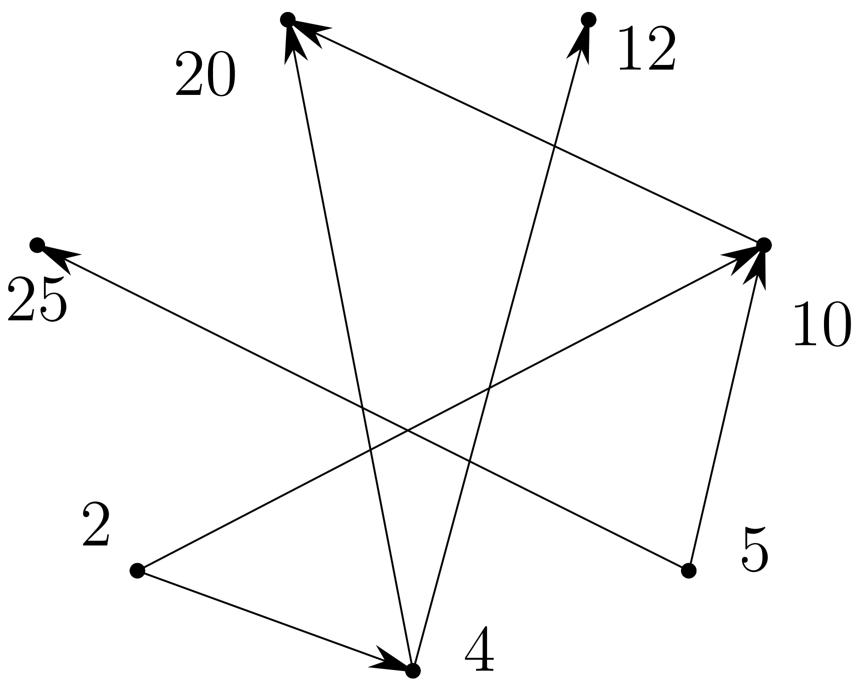


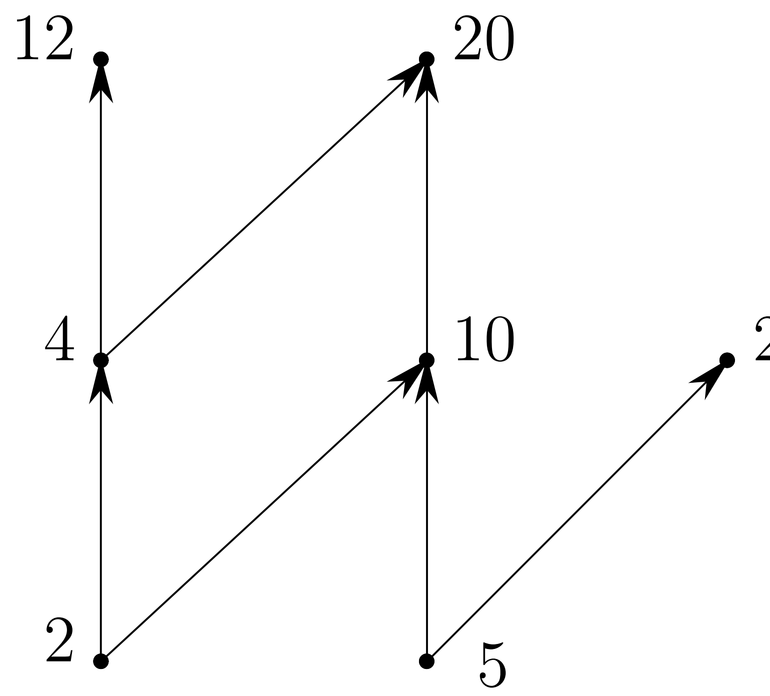
ex :

(2, 4) (4, 20) (2, 20)

Construction du diagramme de Hasse

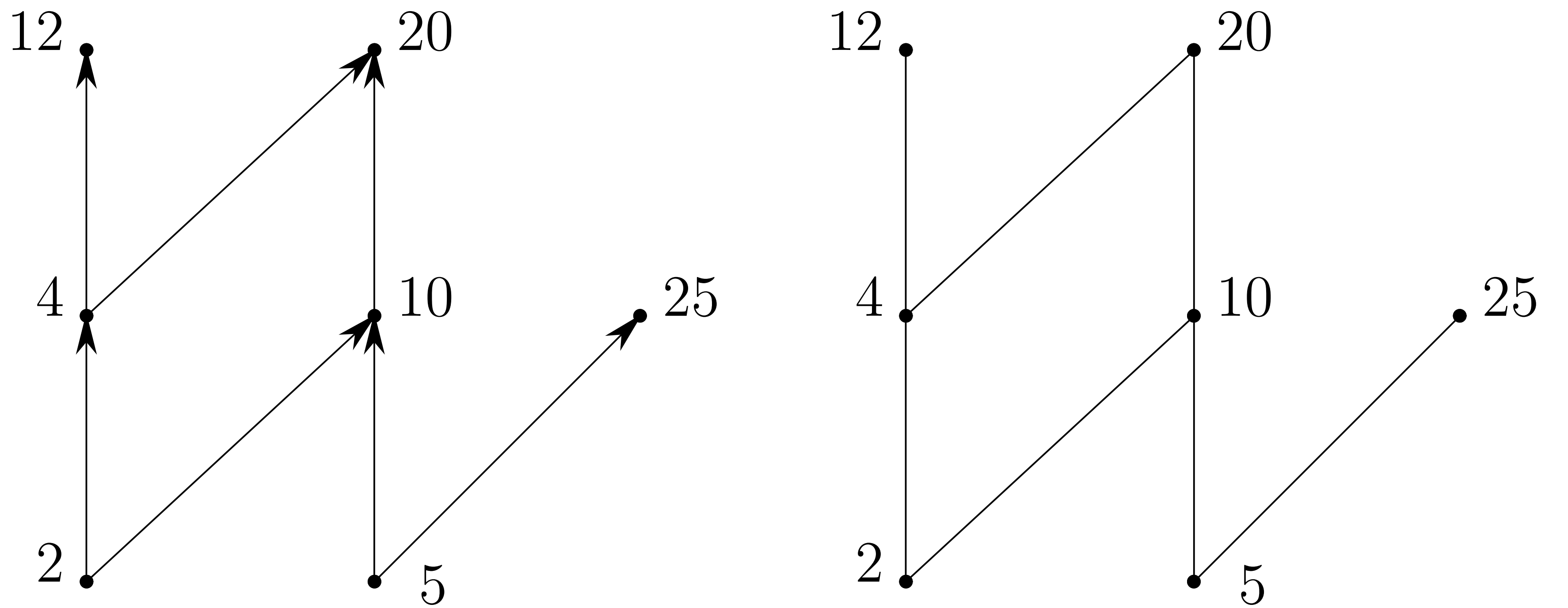
Étape 3 de 4: On dispose chaque arc pour que son sommet initial se situe en dessous de son sommet final.





Construction du diagramme de Hasse

Étape 4 de 4: On retire toutes les flèches sur les arcs orientés puisque tous les arcs pointent vers le haut. Le diagramme de droite est le diagramme de Hasse.



Définitions: élément minimal et maximal

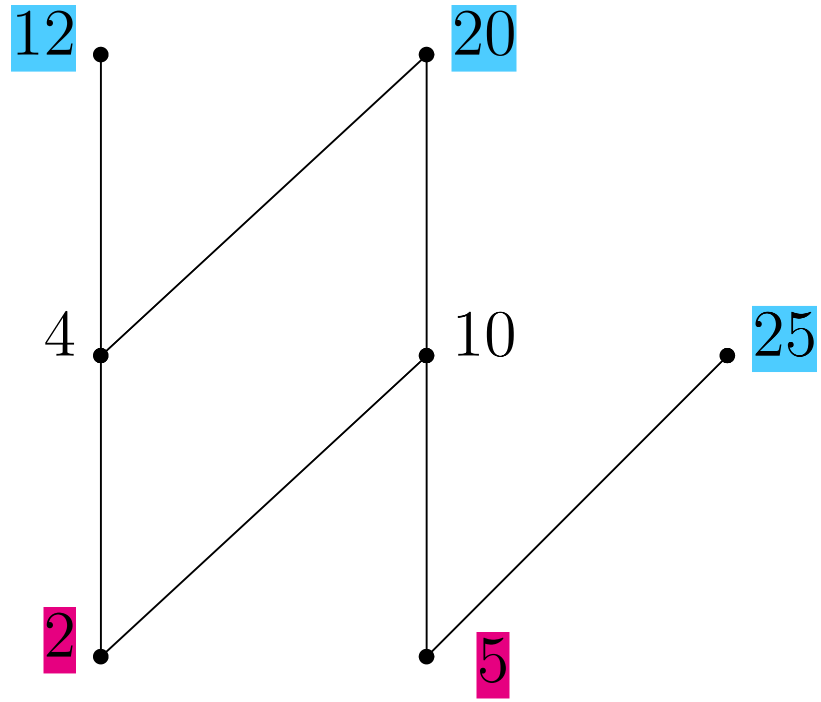
Un élément a d'un ensemble partiellement ordonné $(S, \preccurlyeq)$ est **minimal** s'il n'est pas plus grand que tout élément de l'ensemble partiellement ordonné.

Autrement dit, l'élément $a \in S$ est **minimal** s'il n'y a aucun $b \in S$ tel que $b \prec a$.

Un élément a d'un ensemble partiellement ordonné $(S, \preccurlyeq)$ est **maximal** s'il n'est pas plus petit que tout élément de l'ensemble partiellement ordonné.

Autrement dit, l'élément $a \in S$ est **maximal** s'il n'y a aucun $b \in S$ tel que $a \prec b$.

Exemple $(\{2,4,5,10,12,20,25\},|)$



- 2 et 5 sont les éléments minimaux.
- 12, 20 et 25 sont les éléments maximaux.
- Il peut y avoir plus d'un élément minimal ou maximal dans un ensemble partiellement ordonné.

Exemple $(\{1, 2, 3, 4\}, \leq)$

- 1 est l'élément minimal.
- 4 est l'élément maximal.
- Il peut y avoir au plus un élément minimal ou maximal dans un ensemble totalement ordonné.

Définitions: le plus petit et le plus grand élément

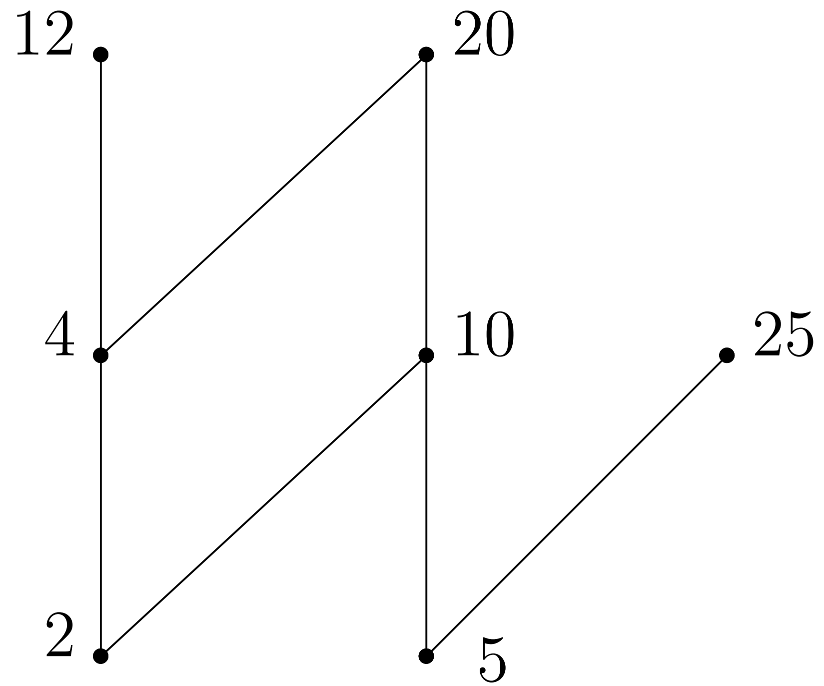
Un élément a d'un ensemble partiellement ordonné $(S, \preccurlyeq)$ est le **plus petit élément** s'il est plus petit que tous les autres éléments.

Autrement dit, l'élément a est le **plus petit élément** de $(S, \preccurlyeq)$ si $a \preccurlyeq b$ pour tout $b \in S$.

Un élément a d'un ensemble partiellement ordonné $(S, \preccurlyeq)$ est le **plus grand élément** s'il est plus grand que tous les autres éléments.

Autrement dit, l'élément a est le **plus grand élément** de $(S, \preccurlyeq)$ si $b \preccurlyeq a$ pour tout $b \in S$.

Exemple $(\{2, 4, 5, 10, 12, 20, 25\}, |)$



- Il n’y a pas de plus petit élément.
- Il n’y a pas de plus grand élément.

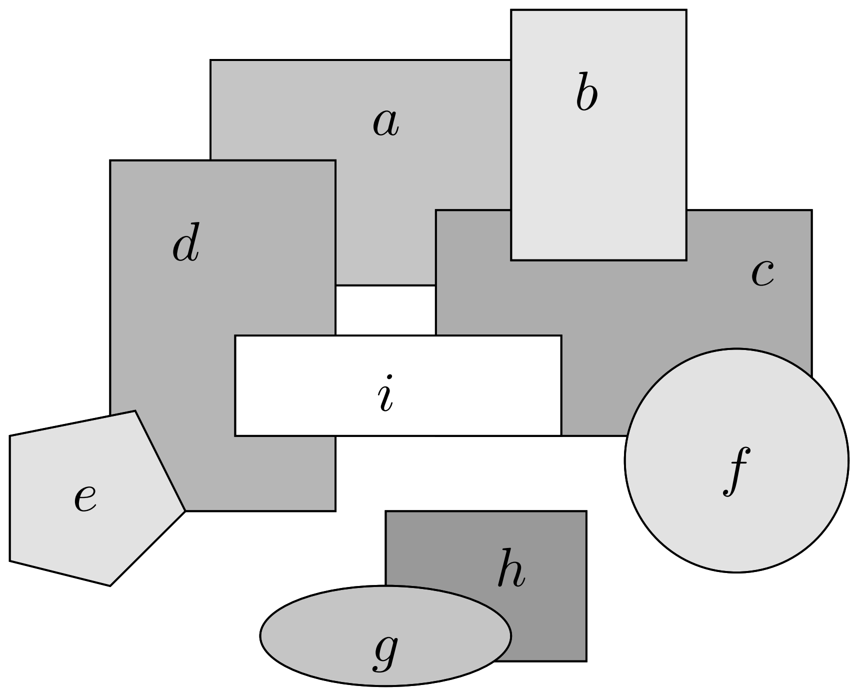
Exemple $(\{1,2,3,4\},\leq)$

- 1 est le plus petit élément.
- 4 est le plus grand élément.

Tri topologique: exemple intro-ductif

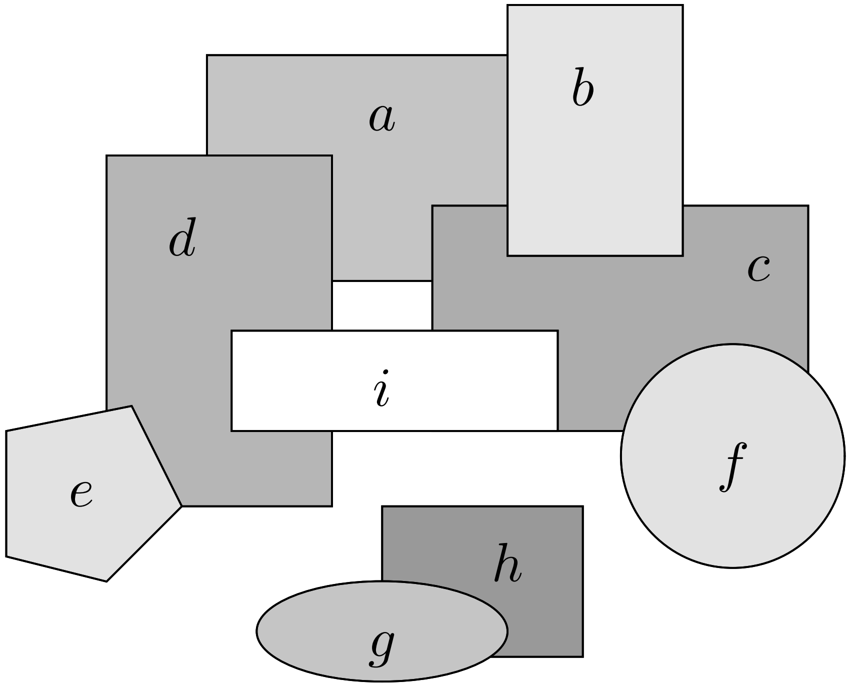
Soit l'ensemble S des formes géométriques $\{a, b, c, d, e, f, g, h, i\}$. Soit la relation R "est plus ou aussi distant que". Alors R est une relation de préordre sur S.

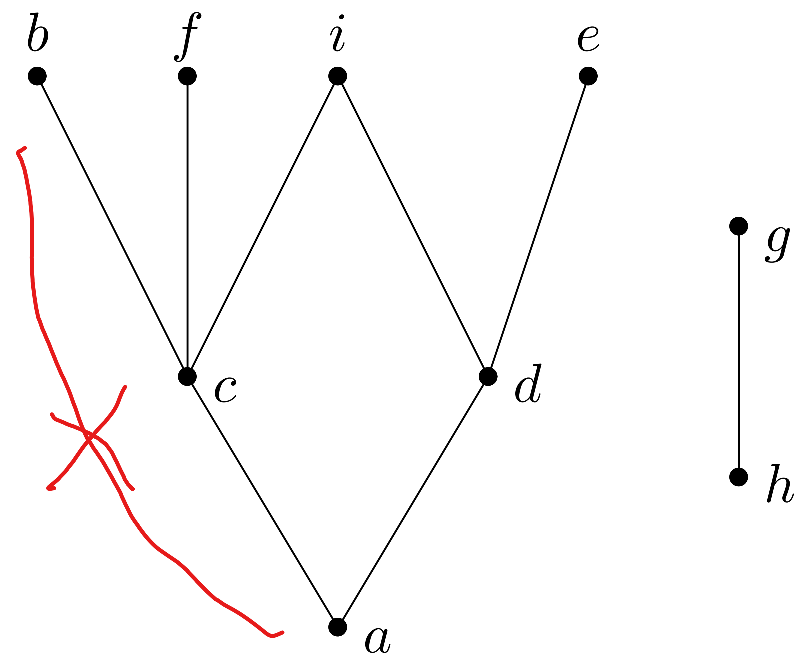
Deux formes géométriques a et b sont en relation, $a\,R\,b$ si a est plus ou aussi distant que b.



Exemple introductif (suite)

La relation
$R = \{(a,c),(a,d),(c,b),(c,f),(c,i),(d,i),$
$(d,e),(h,g)\}$ et son diagramme de Hasse.





Éléments minimaux? Maximaux?

a et h b, f, i, e, g

Définition: ordre compatible et tri topologique

On dit qu'une relation d'ordre total $\preccurlyeq$ est **compatible** avec la relation de préordre R si $a \preccurlyeq b$ lorsque $a\,R\,b$. La formation d'une relation d'ordre total à partir d'une relation de préordre s'appelle le **tri topologique**.

LEMME: Tout ensemble *partiellement ordonné fini* et *non vide* $(S, \preccurlyeq)$ admet un élément minimal.

DÉMONSTRATION: Choisir une élément a_0 de S. Si a_0 n'est pas minimal, il existe a_1 avec $a_1 \prec a_0$. Si a_1 n'est pas minimal, il existe a_2 tel que $a_2 \prec a_1$. Et ainsi de suite. Comme S est fini, ce processus se terminera avec un élément minimal a_n.

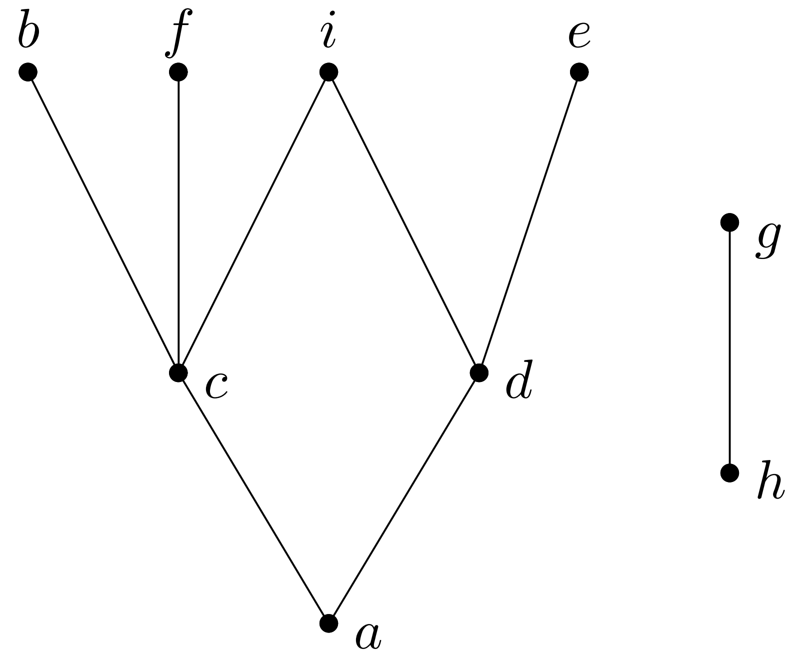
Algorithme de tri topologique

procédure *tri topologique* (S: ensemble partiellement
ordonné fini)
$k := 1$
tant que $S \neq \emptyset$
début
a_k := un élément minimal de S
{cet élément existe selon le lemme}
$S := S - \{a_k\}$
$k := k + 1$
fin
{ $a_1, a_2, \ldots, a_n$ est une relation d'ordre total
compatible de S}

Algorithme de tri topologique

Étape 1 de 9: On choisit l'élément minimal a

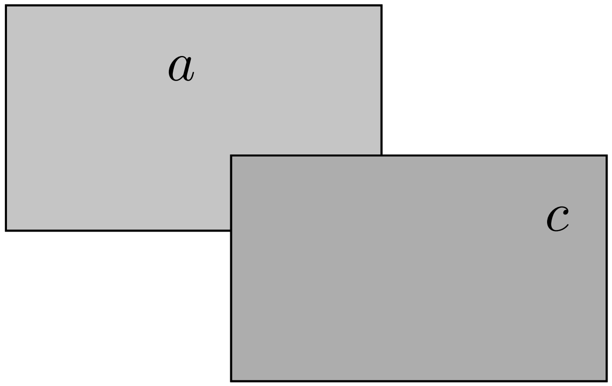
a

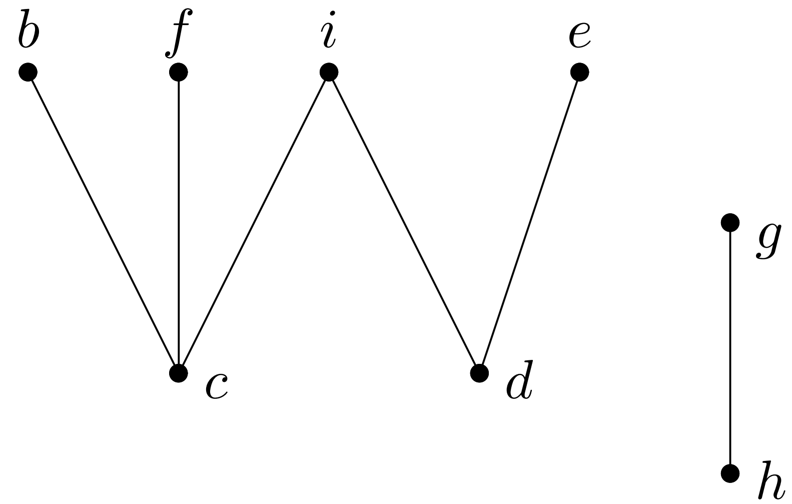


a

Algorithme de tri topologique

Étape 2 de 9: On choisit l'élément minimal c

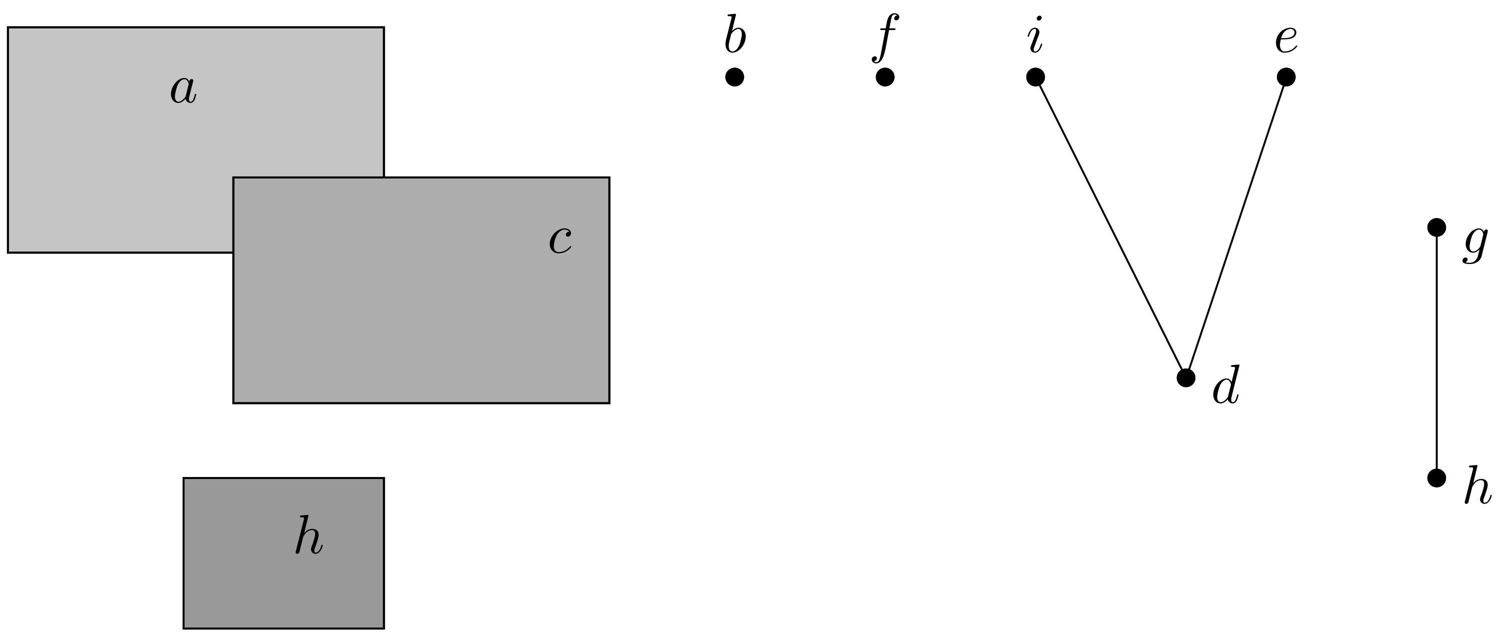




$$a \preccurlyeq c$$

Algorithme de tri topologique

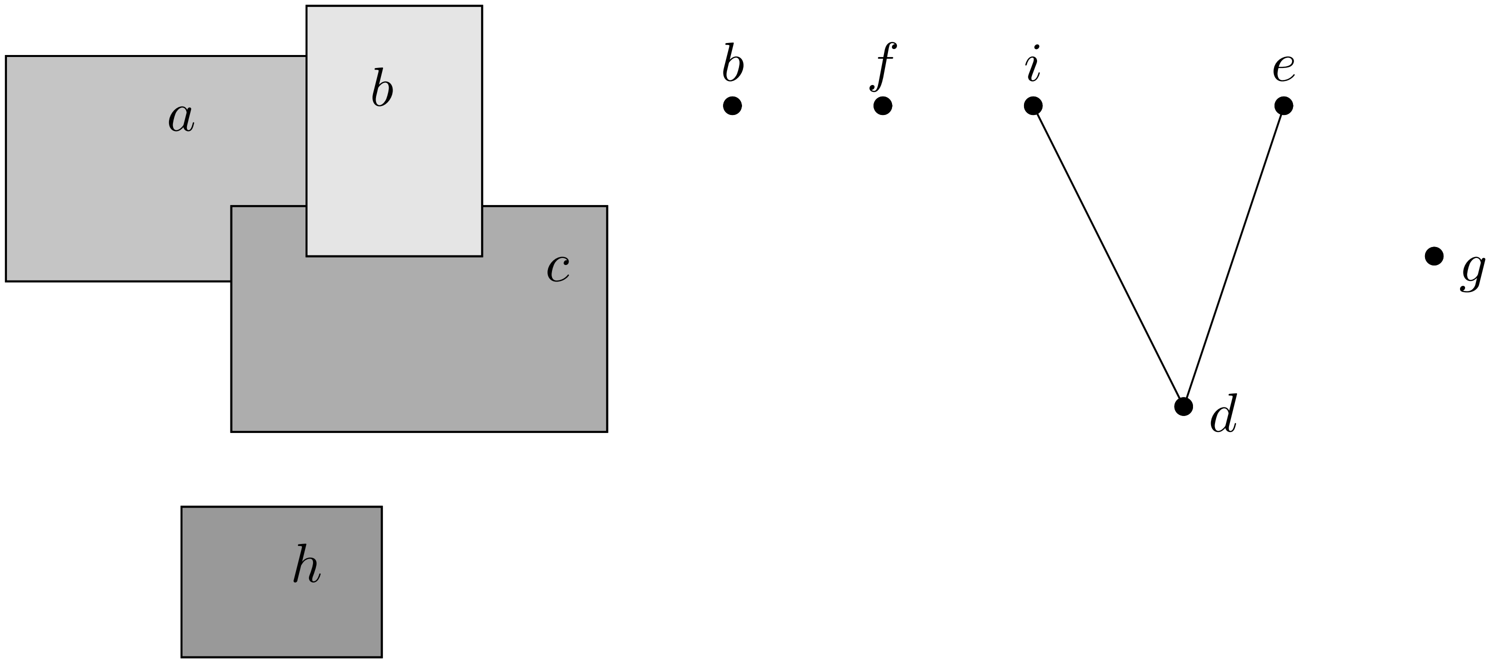
Étape 3 de 9: On choisit l'élément minimal h



$$a \preccurlyeq c \preccurlyeq h$$

Algorithme de tri topologique

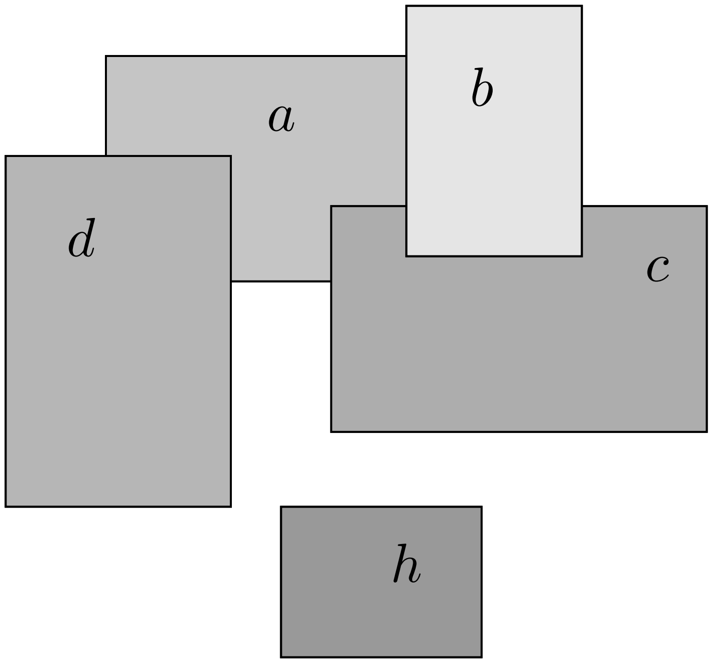
Étape 4 de 9: On choisit l'élément minimal b

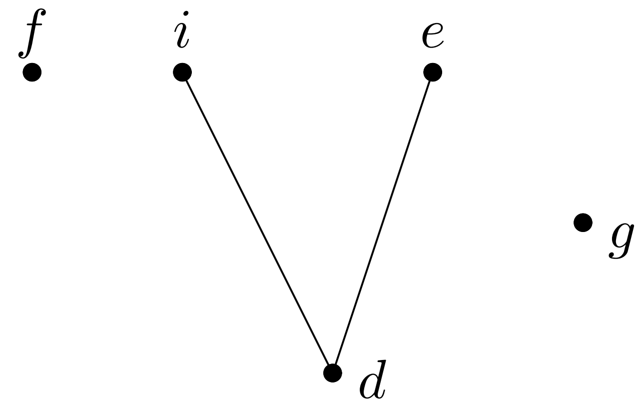


$$a \preccurlyeq c \preccurlyeq h \preccurlyeq b$$

Algorithme de tri topologique

Étape 5 de 9: On choisit l'élément minimal d

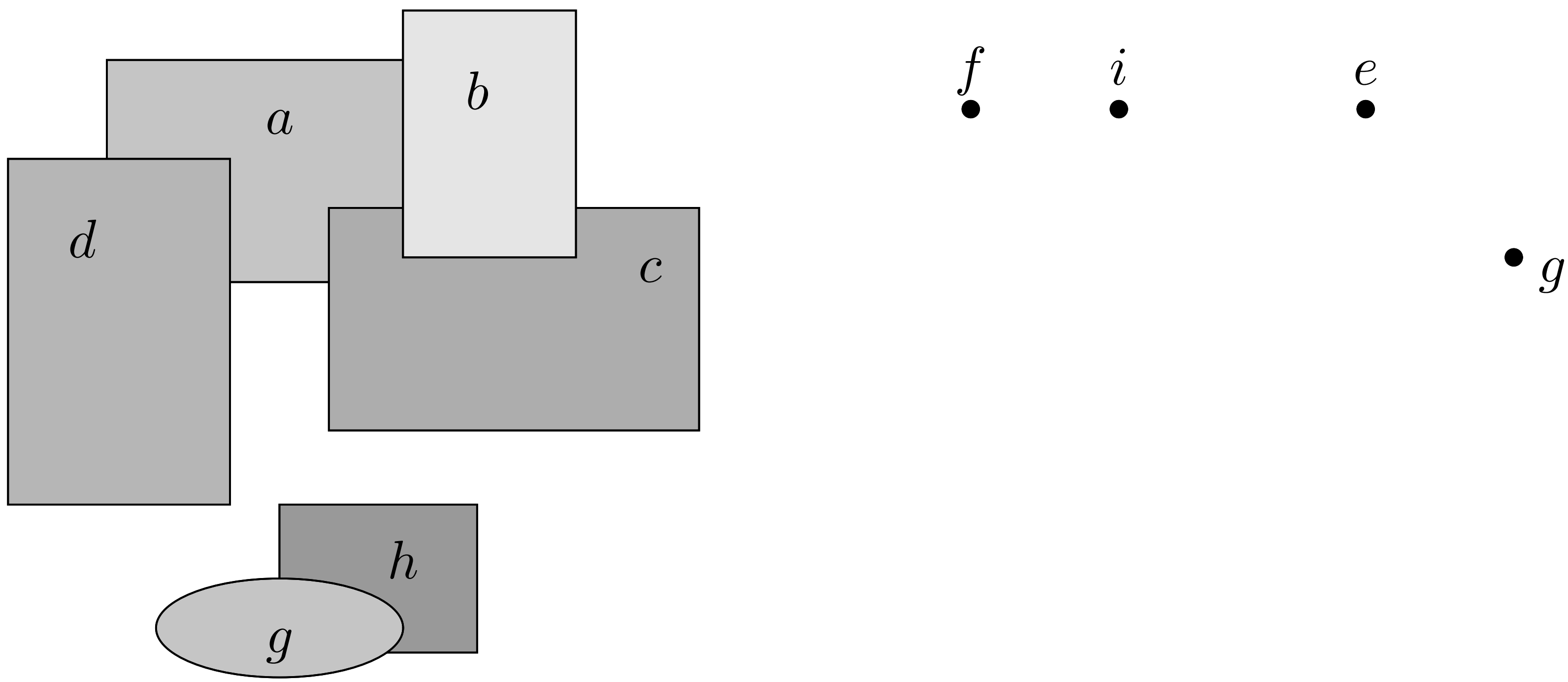




$$a \preccurlyeq c \preccurlyeq h \preccurlyeq b \preccurlyeq d$$

Algorithme de tri topologique

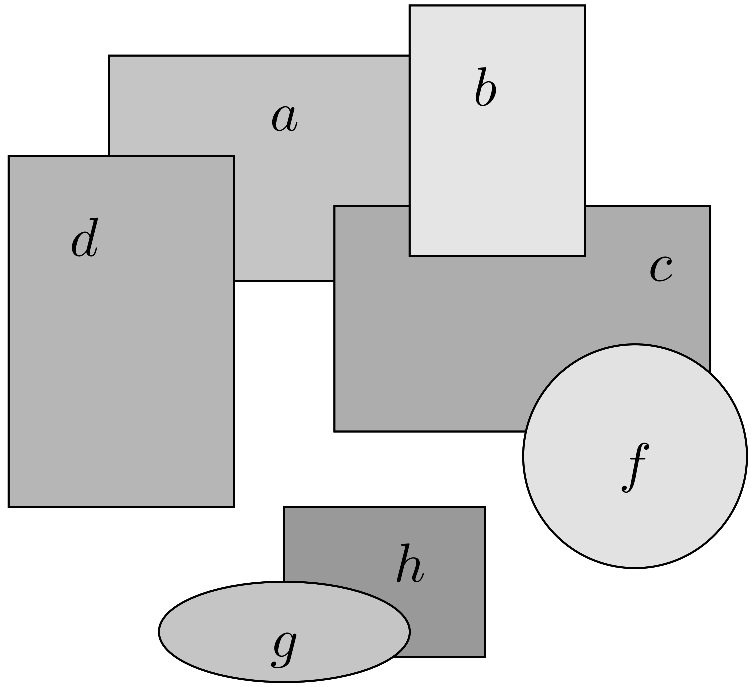
Étape 6 de 9: On choisit l’élément minimal g



$$a \preccurlyeq c \preccurlyeq h \preccurlyeq b \preccurlyeq d \preccurlyeq g$$

Algorithme de tri topologique

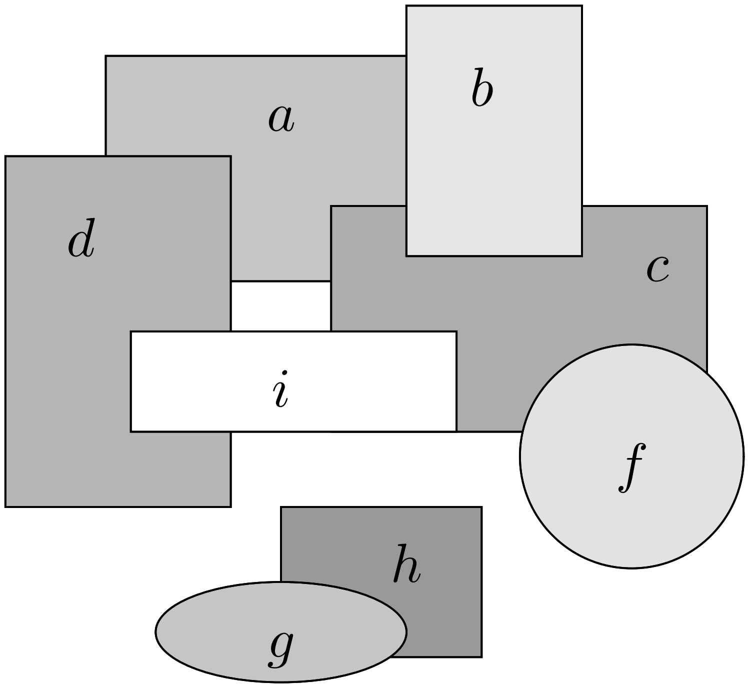
Étape 7 de 9: On choisit l'élément minimal f



$$a \preccurlyeq c \preccurlyeq h \preccurlyeq b \preccurlyeq d \preccurlyeq g \preccurlyeq f$$

Algorithme de tri topologique

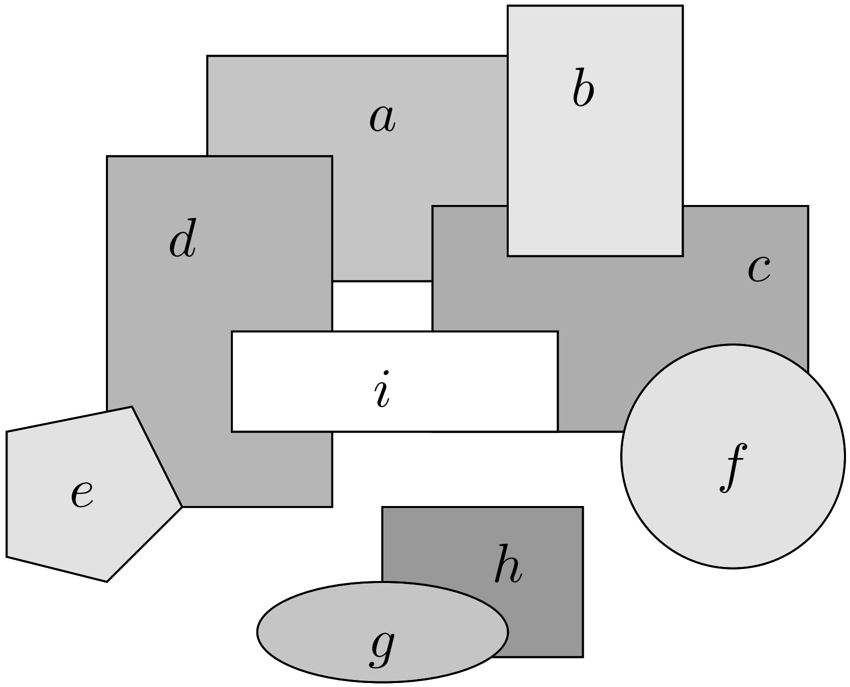
Étape 8 de 9: On choisit l'élément minimal i



$$a \preccurlyeq c \preccurlyeq h \preccurlyeq b \preccurlyeq d \preccurlyeq g \preccurlyeq f \preccurlyeq i$$

Algorithme de tri topologique

Étape 9 de 9: On choisit l'élément minimal e



Ordre total $a \preccurlyeq c \preccurlyeq h \preccurlyeq b \preccurlyeq d \preccurlyeq g \preccurlyeq f \preccurlyeq i \preccurlyeq e$ compatible avec l'ordre partiel $a\,R\,c$, $a\,R\,d$, $c\,R\,b$, $c\,R\,f$, $c\,R\,i$, $d\,R\,i$, $d\,R\,e$, $h\,R\,g$.