Introduction aux mathématiques discrètes

François Schwarzentruber
Université de Rennes 1

Pourquoi cette mise à niveau en mathématiques ?

Plus tard :

- Développeur
- Ingénieur
- Chercheur

Pour avoir les idées claires :

- communiquer ses idées dans un langage mathématique propre
- comprendre les autres,
- raisonner (terminaison d'un programme, etc.)

Introduction

Ce cours est un voyage au pays des mathématiques discrètes.

Bibliographie

- André Arnold, Irène Guessarian. Mathématiques pour l'informatique.
- Alfred Aho, Jeffrey Ullman. Concepts fondamentaux de l'informatique.

Plan

Plan

Syllogismes

On sait que :

- Tous les hommes sont mortels;
- Socrate est un homme.

On en déduit :

- Socrate est mortel.

Démonstration

On sait que :

1. Tous les hommes sont des primates;
2. Tous les mamifères sont mortels et sympas;
3. Tous les primates sont des mamifères;

Theorem

Socrate est un homme alors Socrate est mortel. (on note Socrate est un homme $\Rightarrow$ Socrate est mortel)

Proof.

Supposons que Socrate est un homme. Par 1. Socrate est une primate. Par 3. Socrate est un mamifère. Par 2. Socrate est mortel et sympa, donc en particulier il est mortel. $\square$

Plan

Démonstration
- Implication
- Equivalence

Ensembles

Deux techniques de démonstration

Relations

Logique

Cardinalité

Equivalence

On dit que $A \Leftrightarrow B$ si:

- $A \Rightarrow B$
- $B \Rightarrow A$.

Exercice

On sait que :

1. Tous les hommes sont des primates;
2. Tous les hommes sont intelligents;
3. Tous les primates sont des mamifères;
4. Tous les êtres intelligents sont conscients;
5. Les mamifères conscients sont des hommes;

Montrer que Socrate est un homme ssi Socrate est un mamifère intelligent.

Plan

Démonstration

Ensembles

Deux techniques de démonstration

Relations

Logique

Cardinalité

Plan

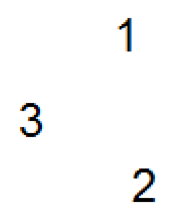
Ensembles - Motivation

Manipulation d'ensembles dans un algorithme :

- Ensemble de chansons
- Jeu vidéo : ensemble des ennemis
- Trajet en train : parcours d'un graphe et ensemble des sommets visités
- etc.

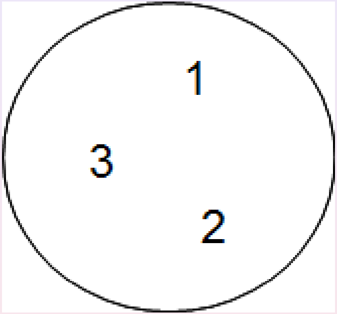
Ensemble

Voici trois entiers, trois éléments...



Ensemble

On crée un ensemble :



Notation : $\{1, 2, 3\}$

Relation entre éléments et ensemble : appartenance

l'élément x appartient à l'ensemble E *ou* x est dans E

Notation

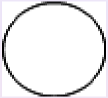
$x \in E$

- $1 \in \{1, 2, 3\}$
  1 appartient à l'ensemble $\{1, 2, 3\}$
- $4 \notin \{1, 2, 3\}$
  4 n'appartient pas à l'ensemble $\{1, 2, 3\}$

Des ensembles... on peut en créer pleins !

- $\{1, 2, 3, 5\}$
- $\{3, 6\}$
- $\{1\}$
- $\{1, \ldots, 100\}$
- $\mathbb{N}$ (ensemble des entiers naturels)

L’ensemble vide



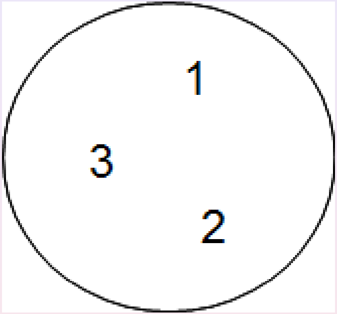
Notation

$\emptyset$

Remarque

Pour tout élément x, on a $x \notin \emptyset$!

Ensemble : l'ordre n'a pas d'importance



$\{1, 2, 3\}$ $\{1, 3, 2\}$ $\{2, 1, 3\}$ $\dots$

Définition en intension

Notation

Ensemble des éléments de A qui vérifient la propriété P :
$\{x \in A \mid P(x)\}$

$\{x \in \mathbb{N} \mid x \text{ est pair}\}$
$\{x \in \mathbb{N} \mid x \text{ est impair}\}$

Egalité de deux ensembles

Definition

Deux ensembles sont égaux s'ils contiennent les même éléments.

Notation

$A = B$

- $\{1, 2, 3\} = \{2, 1, 3\}$
- $\{1, 2\} = \{1, 2\}$
- $\{1, 2\} \neq \{1, 2, 3\}$

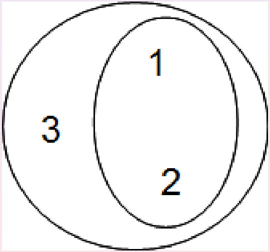
Inclusion entre ensembles

Definition

L'ensemble A est inclu dans l'ensemble B si tous les éléments de A sont dans B.

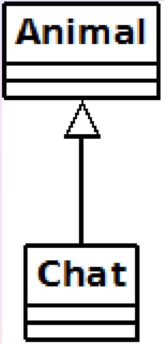
Notation

$A \subseteq B$



- $\{1, 2\} \subseteq \{1, 2, 3\}$

Héritage et inclusion



Si la classe Chat hérite de la classe Animal, alors l'ensemble des instances de Chat est inclus dans l'ensemble des instances de Animal.

Cardinalité

Definition

Soit A un ensemble fini. Le cardinal de A est le nombre d'éléments dans A.

Exemple

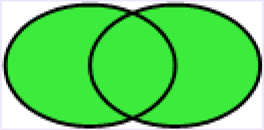
- $card(\{1, 4, 456\}) = 3;$
- $card(\{1, 4, 456, 5, 6\}) = 5.$

Mise au point

- Pour tout ensemble A on a $\emptyset \subseteq A$
- $A \subseteq B$ et $B \subseteq A$ si, et seulement si $A = B$.

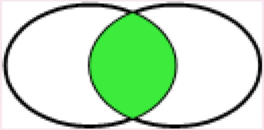
Plan

Union et intersection



- Union : "on prend tout"
  $\{1, 2\} \cup \{2, 3\} = \{1, 2, 3\}$

- Intersection : "on prend ce qui est commun"
  $\{1, 2\} \cap \{2, 3\} = \{2\}$



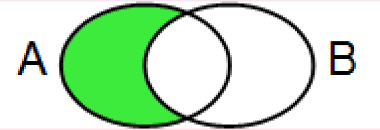
Complémentaire

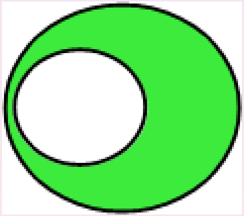
Definition

A privé de *B* est l'ensemble des éléments de *A* qui ne sont pas dans *B*.

Notation

$A \setminus B$





Complémentaire - exemples

- $\{1, 2, 3\} \setminus \{1, 2\} = \{3\}$
- $\mathbb{N} \setminus \{1, 2, 3\}$: ensemble des entiers naturels qui ne sont ni 1, ni 2 et ni 3.

Algèbre

- $S \cup T = T \cup S$;
- $S \cup (T \cup R) = (S \cup T) \cup R$;
- $S \cap T = T \cap S$;
- $S \cap (T \cap R) = (S \cap T) \cap R$;
- $S \cap (T \cup R) = (S \cap T) \cup (S \cap R)$;
- $S \cup (T \cap R) = (S \cup T) \cap (S \cup R)$;
- $S \setminus (T \cup R) = (S \setminus T) \setminus R$;
- $(S \cup T) \setminus R = (S \setminus R) \cup (T \setminus R)$
- $S \cup \emptyset = S$;
- $S \cup S = S \cap S = S$

Exercices

Exercice

Montrer que

$$A \subseteq B \Leftrightarrow A \cap B = A \Leftrightarrow A \cup B = B$$

.

Exercice

Montrer que

$$A = B \Leftrightarrow A \cup B = A \cap B$$

.

Plan

Couple

$(3, 5)$ est un couple composé :

- d'une première coordonnée égale à 3 ;
- d'une deuxième coordonnée égale à 5.

Produit cartésien

Le produit cartésien de A et B est l'ensemble des couples (x, y) où $x \in A$ et $y \in B$.

Notation

$A \times B$

$\mathbb{N} \times \mathbb{N}$ est l'ensemble des couples d'entiers.
$\{1, 2\} \times \{3, 4, 5\} = ...$

Exercice

Exercice

Résoudre l'équation $A \times B = \emptyset$.

Exercice

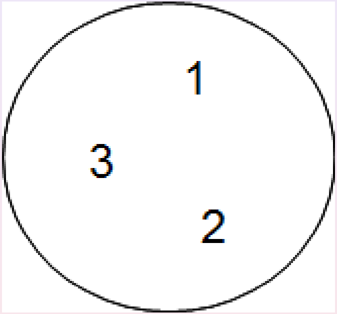
- *A-t-on* $(A \cap B) \times (C \cap D) =^? (A \times C) \cap (B \cap D)$?
- *A-t-on* $(A \cup B) \times (C \cup D) =^? (A \times C) \cup (B \cap D)$?

(donner une démonstration ou un contre-exemple)

Plan

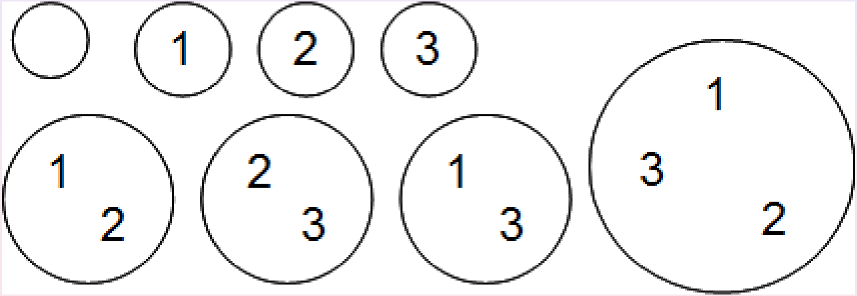
Parties d'un ensemble

Quels sont les sous-ensembles de ça ?



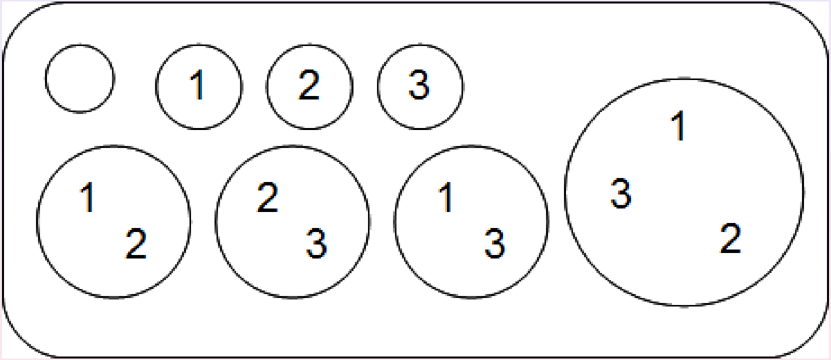
Parties d’un ensemble

Il y en a six :



$\emptyset$ $\{1\}$ $\{2\}$ $\{3\}$ $\{1,2\}$ $\{2,3\}$ $\{1,3\}$ $\{1,2,3\}$

Ensemble des parties d'un ensemble



$$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

Ensemble des parties d'un ensemble

Definition

$P(A)$ est l'ensemble des ensembles inclus dans A.

$$P(\{1,2,3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{2,3\}, \{1,3\}, \{1,2,3\}\}$$

$A \subseteq B$ ssi $A \in P(B)$

A vous de jouer !

- $P(\{1,2\}) = ...$
- $P(\{1\}) = ...$
- $P(\emptyset) = ...$
- $P(P(\{1\})) = ...$
- $P(P(P(\emptyset))) = ...$

- Expliquer $x \in P(E)$, $x \subseteq P(E)$ et $x \subseteq E$.

Plan

Interface

Ensemble E

- Ajouter un élément : $E := E \cup \{x\}$
- Supprimer un élément : $E := E \setminus \{x\}$
- Tester l'appartenance : $x \in E$

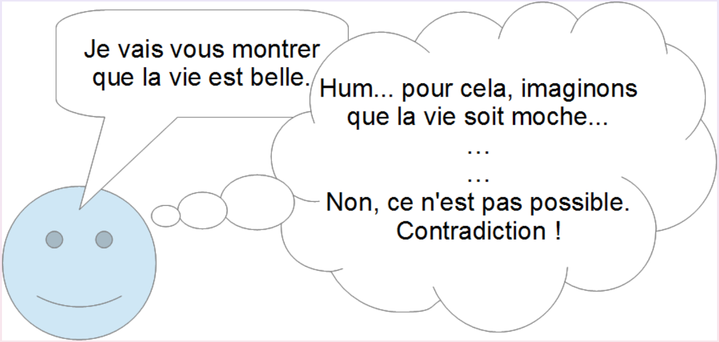
Implémentations

- Tableau
- Tableau trié
- Listes
- Listes triées
- Arbres binaires de recherche (équilibrés)
- Vecteurs caractéristiques
- Tables de hâchage

Plan

Plan

Raisonnement par l'absurde



Plan

Récurrence - induction. Motivation

En informatique, on manipule des structures inductives :

- Listes
- Arbres (rouges et noirs, arbres syntaxiques, etc.)
- Programmes LISP, JAVA etc.
- Squelette animé

On veut :

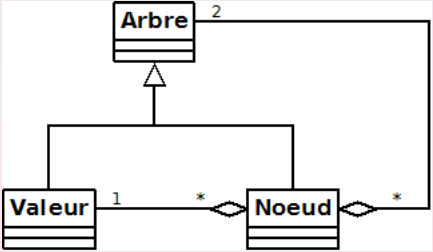
- Définir un objet inductif
- Démontrer des propriétés

Exemple : arbres binaires d'entiers

Definition

Soit V un ensemble. On définit l'ensemble A des arbres comme le plus petit ensemble tel que :

- $V \subseteq A$;
- Si $a_1, a_2 \in A$ et $v \in V$, alors $noeud(v, a_1, a_2) \in A$.



Récurrence - Induction

- Cas de base : Je montre $P(0)$...
- Cas récursif : Soit $k \in \mathbb{N}$. Supposons $P(k)$. Je montre $P(k+1)$...
- Par récurrence, j'ai montré que pour tout $k \in \mathbb{N}$, $P(k)$ est vraie.

–

- Cas de base : Je montre $P(v)$ pour $v \in V$.
- Cas inductif : Soit $a_1, a_2 \in A$ pour lesquels je suppose $P(a_1)$ et $P(a_2)$. Soit $v \in V$ Je montre $P(noeud(v, a_1, a_2))$...
- Par induction, j'ai montré que pour tout $a \in A$, $P(a)$ est vraie.

A vous de jouer !

Soit $f(x) = \frac{1}{3}x^3 + ax^2 + bx$.

- Trouver a et b tels que $\forall x \in \mathbb{R}$, $f(x+1) - f(x) = x^2$. Dans la suite, cette propriété est vérifiée.
- Montrer que $\forall n \in \mathbb{N}$, $f(n)$ est un entier.
- Montrer que pour tout $n \in \mathbb{N}$, $\Sigma_{k=0}^{n} k^2 = f(n+1) = \frac{n(n+1)(2n+1)}{6}$.

Soit a un arbre binaire. Donner une inégalité entre le nombre de noeud dans a et la hauteur de a.

Plan

Plan

Relations

Definition

Une relation entre A et B est un sous-ensemble de $A \times B$.

Relations

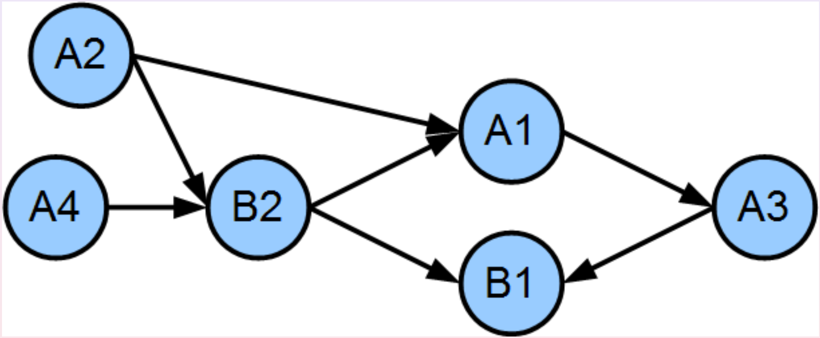
Definition

Une relation sur A est un sous-ensemble de $A \times A$.

- Relation d'amitié dans un réseau social
- Lien entre pages web
- Graphe sémantique d'un mot
- Etat d'une machine $s \rightarrow^{x:=x+1} s'$
- Etats mentaux en psychologie/philosophie (sémantique de Kripke)

Graphe

Une relation sur A est un sous-ensemble de $A \times A$... c'est un graphe !



Plan

Ordre (partiel)

Definition

Un ordre sur E est une relation $\leq$ sur E :

- réflexive : pour tout $x \in E$, $x \leq x$;
- antisymétrique : pour tout $x, y \in E$, $x \leq y$ et $y \leq x$ implique $x = y$;
- transitive : pour tout $x, y, z \in E$, $x \leq y$ et $y \leq z$ implique $x \leq z$.

Exemple :

- l'inclusion ;
- 'être un préfixe de' (utilisée dans les algorithmes de recherche dans une chaîne de caractères)
- 'divise'

Ordre total

Definition
Un ordre total sur E est un ordre $\leq$ sur E tel que pour tout $x, y \in E$, $x \leq y$ ou $y \leq x$.

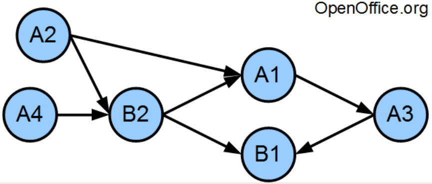
Exemple :

- $\leq$ sur les entiers, réels etc.
- ordre lexicographique sur les mots

Application : tableur

	A	B	C
1	=A2+B2 16	=A3+B2 29	
2	3	=A2+A4 13	
3	=A1 16		
4	10		
5			

OpenOffice.org Calc

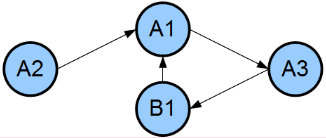


61/104

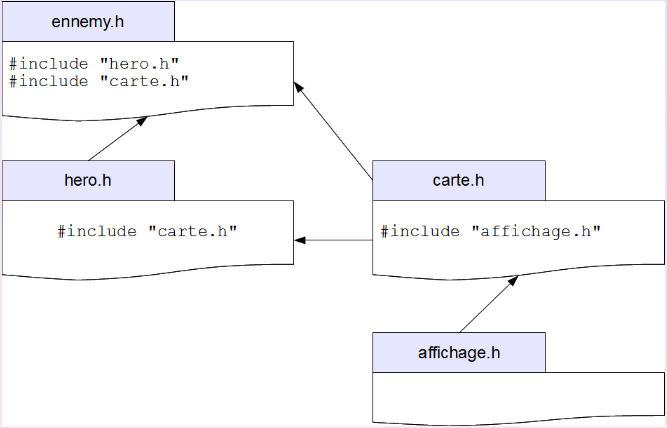
Application : tableur

	A	B	C
1	=A2+B1 Err :522	=A3 Err :522	
2	2		
3	=A1 Err :522		
4			
5			

OpenOffice.org Calc

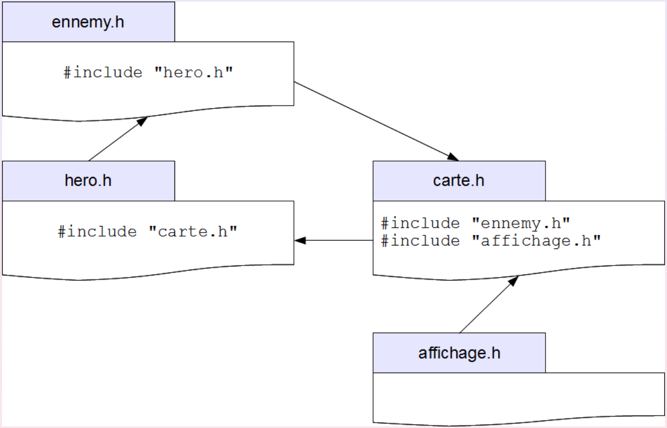


Application : compilation, liaison



63/104

Application : compilation, liaison



Majorant, borne supérieure, maximum

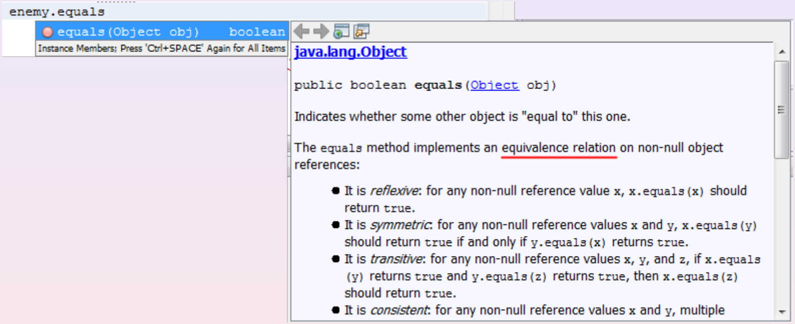
Soit $(E, \leq)$ un ensemble ordonné et $A \subseteq E$.

- M est un *majorant* de A ssi $\forall x \in A$, $x \leq M$.
- M est le *maximum* de A ssi M est un majorant de A et $M \in A$. (unicité du maximum s'il existe).

(définition analogue pour minorant et minimum)
La borne supérieure de A est le minimum de l'ensemble des majorants (s'il existe). (définition analogue pour borne inférieure)

Plan

Motivation : relation d’équivalence



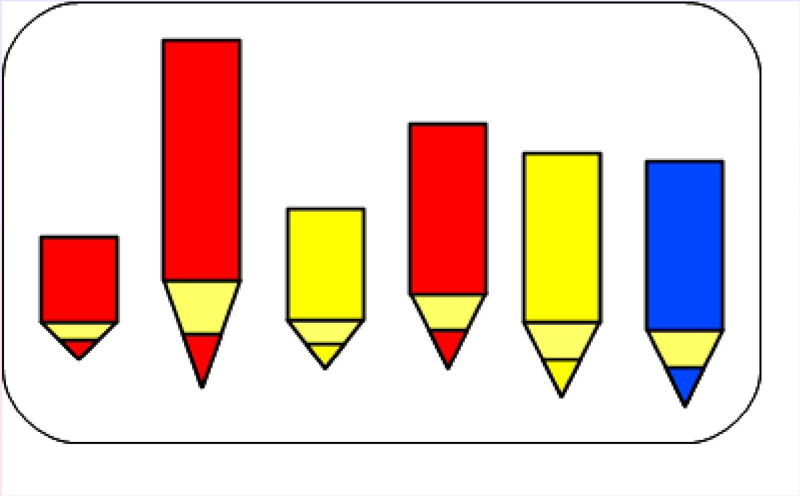
Motivation : relation d’équivalence

C’est un peu une "égalité faible".

- la méthode `equals` en JAVA
- ‘Avoir la même image par une fonction de hâchage’
- les nombres rationnels

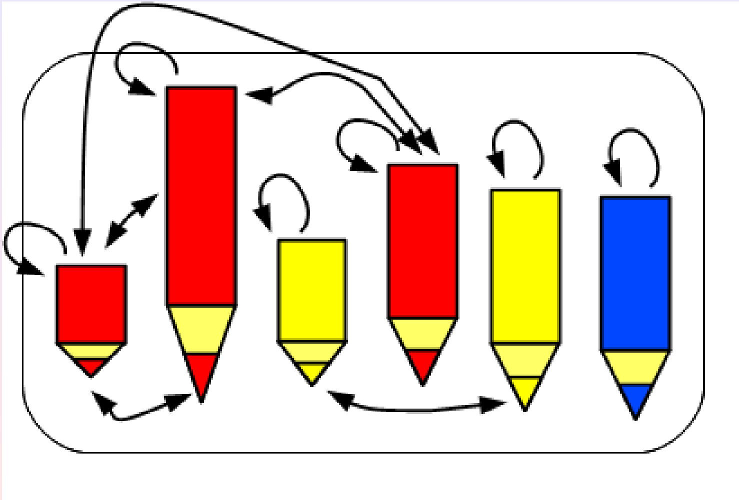
Relation d'équivalence

'Avoir la même couleur' sur cet ensemble de crayons



Relation d'équivalence

'Avoir la même couleur' sur cet ensemble de crayons



Relation d'équivalence

C'est un peu une "égalité faible".

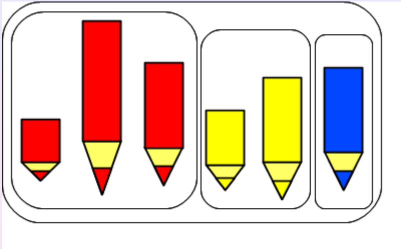
Definition

La relation R sur E est une relation d'équivalence ssi

- R est réflexive : $\forall x \in E, xRx$
- R est transitive : $\forall x, y, z \in E$, (xRy et yRz) implique xRz
- R est symétrique : $\forall x, y \in E$, xRy implique yRx

Ensemble quotient

E/R



- Classe d'équivalence = ensemble d'éléments qui sont équivalents.
- Un représentant d'une classe est un élément de cette classe.
- Les classes d'équivalence forment une partition.

Exemple : construction des nombres rationnels

$\mathbb{Z} \times \mathbb{Z}*$

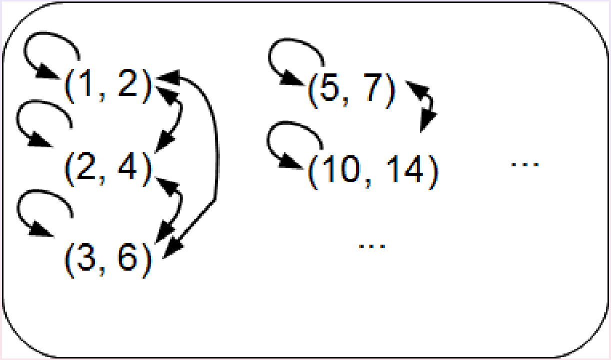
(1, 2) (5, 7)

(2, 4) (10, 14) ...

(3, 6) ...

Exemple : les nombres rationnels

$\mathbb{Z} \times \mathbb{Z}*$

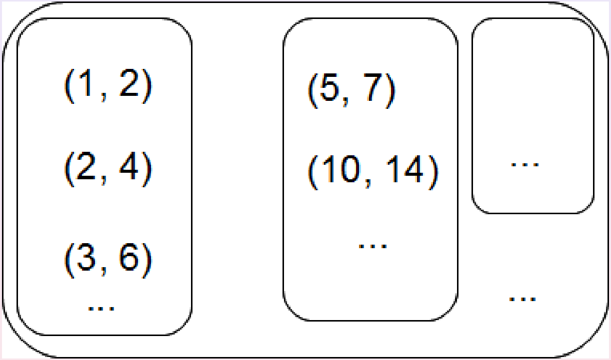


$(a, b)R(x, y)$ ssi $ay = bx$.

74/104

Exemple : les nombres rationnels

$$\mathbb{Q} = \mathbb{Z} \times \mathbb{Z}*/R$$



$(a, b)R(x, y)$ ssi $ay = bx$.

Exemple : les nombres rationnels

```
public class Rationnel
{
    public int getNum() {...}
    public int getDenom() {...}

    @Override
    public boolean equals(Object obj) {
      if(obj instanceof Rationnel)
         return getNum() * obj.getDenom()
                 == getDenom() * obj.getNum();
      else
         return false;
      }
}
```

Exemple : les nombres rationnels... à vous de jouer !

Montrer que la relation R définie sur $\mathbb{Z} \times \mathbb{Z}*$ par $(a, b)R(x, y)$ ssi $ay = bx$ est une relation d'équivalence.

Structure de données pour une relation d'équivalence

Interface :

- Tester si x est équivalent à y (find) ;
- Fusionner deux classes d'équivalence (union).

Implémentation :

- Tableaux avec des numéros de classes d'équivalence ;
- Arbre binaire (structure Union-Find).

Plan

Motivation de la logique

- Architecture
- Résoudre une classe de problèmes (Sudoku, planification, etc.)
- Vérification de programmes / de circuits
- Vérification de démonstration

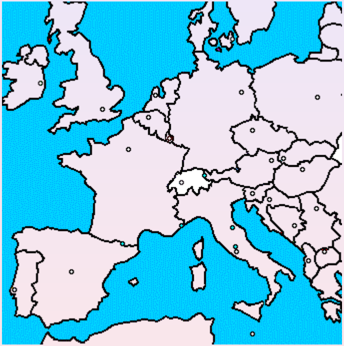
Plan

Résolution de problèmes avec la logique des propositions

- Propositions... ‘la case $(2, 3)$ du sudoku contient un 8’ ;
- $\varphi_1 \wedge \varphi_2$: ET ;
- $\varphi_1 \vee \varphi_2$: OU ;
- $\neg\varphi$: NEGATION.

Résolution de problèmes avec la logique des propositions

	4				2		1	9
			3	5	1		8	6
3	1			9	4	7		
	9	4						7
2						8	9	
		9	5	2			4	1
4	2		1	6	9			
1	6		8				7	



$\rightarrow$ Démonstration avec SAToulouse

Plan

Théorie des ensembles

Applications :

- Vérification de démonstrations par ordinateur
  `http://us.metamath.org/`

De la lecture :

- Cori, Lascar. Logique mathématique.
- BD Logicomix.

Paradoxe de Russell

Gottlob Frege - Bertrand Russell. Correspondance. Juin 1902-décembre 1904 - mars-juin 1912.

Theorem

Il n'existe pas d'ensemble E qui contient tous les ensembles.

Proof.

Supposons qu'il existe un ensemble E qui contient tous les ensembles.
Soit $A = \{X \in E \mid X \notin X\}$
On a ($A \in A$ ssi $A \notin A$). $\square$

Plan

Logique du premier ordre

- $\forall x.\varphi(x)$. Pour tout x, $\varphi(x)$ est vraie.
- $\exists x.\varphi(x)$. Il existe un x tel que $\varphi(x)$ est vraie.

Plan

Liens avec les ensembles

- Intersection, et, pour tout...
  $\{x \in A \mid P(x)\} \cap \{x \in A \mid Q(x)\} = \{x \in A \mid P(x) \wedge Q(x)\}$

  $\bigcap_{i \in I} \{x \in A \mid P_i(x)\} = \{x \in A \mid \forall i \in I, P_i(x)\}$

- Union, ou, il existe...
  $\{x \in A \mid P(x)\} \cup \{x \in A \mid Q(x)\} = \{x \in A \mid P(x) \vee Q(x)\}$

  $\bigcup_{i \in I} \{x \in A \mid P_i(x)\} = \{x \in A \mid \exists i \in I, P_i(x)\}$

Plan

Motivation

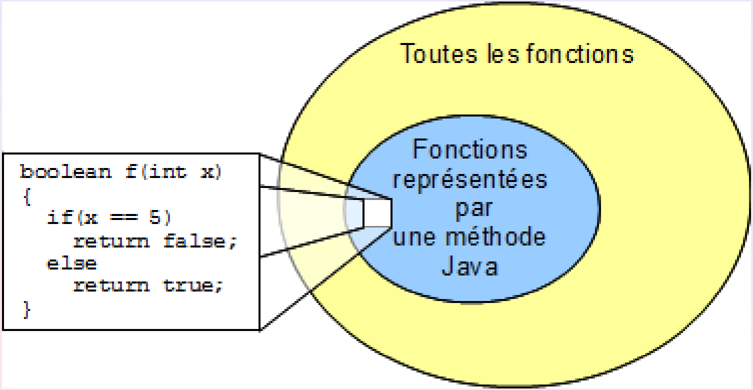
Informatique : art de représenter des objets infinis avec une structure finie...

- Expression régulière $*.txt$ dans grep ;
- Fonction JAVA *int* $\rightarrow$ *boolean*.

Question

Est-ce qu'on est capable de tout représenter ?

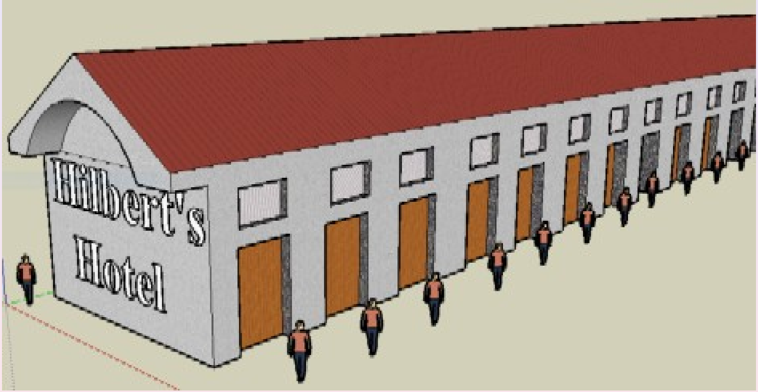
Motivation



Toutes les fonctions
Fonctions représentées par une méthode Java
boolean f(int x)
{
if(x == 5)
return false;
else
return true;
}

Plan

L'hôtel de Hilbert



Plan

Fonction

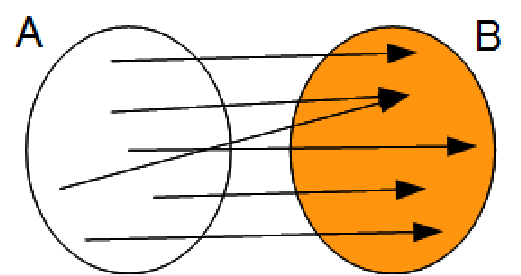
Soit A et B deux ensembles.
$f : A \to B$ associe à tout élément de A un élément de B.

Example

$$f : \begin{array}{ccc} \mathbb{N} & \to & \mathbb{N} \\ x & \mapsto & x + 1 \end{array}$$

Fonction surjective

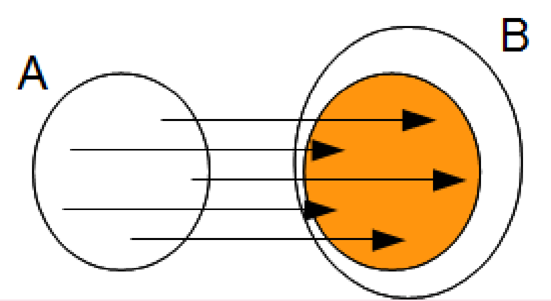
Tous les éléments de B sont atteints.
$\forall b \in B, \exists a \in A \mid b = f(a)$



'A a plus d'éléments que B'.

Fonction injective

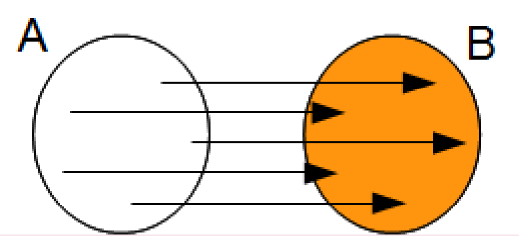
Une image n'a au plus qu'un antécédent.
$\forall a_1, a_2 \in A, f(a_1) = f(a_2) \Rightarrow a_1 = a_2$



'A a moins d'éléments que B'

Fonction bijective

Tout élément de B a un unique antécédent.
$\forall b \in B, !\exists a \in A \mid b = f(a)$



'A a 'autant' d'éléments que B'

Plan

Dénombrabilité

Definition

Un ensemble E est dénombrable si il existe une bijection $f : \mathbb{N} \to E$.

Exemple :

- $\mathbb{N}$ est dénombrable.
- $\mathbb{N} \times \mathbb{N}$ est dénombrable.
- L'ensemble des mots finis sur $\{a, b, \dots, z\}$ est dénombrable.
- L'ensemble des fonctions Java *int* $\to$ *boolean* est dénombrable.
- L'ensemble des mots finis sur $\mathbb{N}$ est dénombrable.

Plan

A vous de jouer !

Theorem

Démontrer que l'ensemble $P(\mathbb{N})$ n'est pas dénombrable.