

## Mathématiques pour l'Informatique

Vers l'infini

David Teller

23/01/2007

## Jusqu'à présent

Nous avons déjà abordé

Les ensembles Le regroupement de valeurs caractérisées par des critères.

Informatique Types.

Physique Unités.

Logique Domaines.

Linguistique Rôles grammaticaux.

...

Les fonctions Les traitements et transformations qu'on peut apporter à ces valeurs.

Informatique Programmes.

Logique Théorèmes.

Linguistique Compréhension.

...



## Au programme

**Cardinalité** Mesurer la taille d'un ensemble – c'est-à-dire déjà déterminer si l'on a les outils pour en parler.

**Relations** Être en mesure de parler des propriétés d'une valeur.

## Introduction

## Cardinalité

Ensembles finis

Ensembles dénombrables

## Relations

Opérations

Relations



## Conclusions



## Le problème de la cardinalité

Le **problème** Étant donné un ensemble de valeurs  $E$ , sait-on le manipuler ?

La **réponse** Cela va dépendre essentiellement de deux choses

- ▶ dispose-t-on d'une axiomatisation de  $E$  ?
- ▶ l'ensemble  $E$  est-il dénombrable, voire fini ?



## Ensemble fini

## Definition (Ensemble fini)

Un ensemble  $E$  est dit *fini* s'il existe un entier  $n$  et une bijection entre  $f : E \rightarrow [n]$ . On dit alors que son *cardinal* est  $n$  et l'on note  $|E| = n$ .

## Exercice (Booléens)

*Prouver que l'ensemble des booléens  $\mathbf{B} = \{\text{ff}, \text{tt}\}$  est fini. Quel est le cardinal de  $\mathbf{B}$  ?*



## Segments entiers

Pour tout entier  $n$  de  $\mathbf{N}$ , on notera  $[n]$  l'ensemble  $\{1, 2, \dots, n\}$ .

## Proposition

*Si  $n < m$  alors il n'existe pas d'injection de  $[m]$  vers  $[n]$ .*

**Exercice** Prouvez-le. Vous pourrez utiliser une récurrence sur  $m$ .

## Quelques propriétés

## Proposition (Partition)

*Si  $E$  est un ensemble fini et si  $(A_i)_{i \in I}$  est une partition de  $E$ , alors*

- ▶ chaque  $A_i$  est un ensemble fini
- ▶  $|E| = \sum_{i \in I} |A_i|$

**Exercice** Prouvez cela.

## Proposition (Bijections entre ensembles finis)

*Si  $E$  et  $F$  sont deux ensembles finis de même cardinal, il existe une bijection entre  $E$  et  $F$ .*



## Avant de généraliser

### Proposition (Injection/surjection)

Soient  $E$  et  $F$  deux ensembles quelconques. Il existe une application injective de  $E$  vers  $F$  si et seulement si il existe une application surjective de  $F$  vers  $E$ .

**Preuve (si)** Considérons une application surjective  $g : F \rightarrow E$ . Comme  $g$  est une application surjective,  $g$  admet un inverse à droite, c'est-à-dire une application  $s$  telle que  $g \circ s = Id_E$ .

Nous savons que  $s$  est une application, prouvons que  $s$  est injective. Considérons  $x$  et  $y$  tels que  $s(x) = s(y)$ . Alors,  $g(s(x)) = g(s(y))$ . Or,  $g(s(x)) = x$  et  $g(s(y)) = y$ . Par conséquent,  $x = y$ . Comme ceci est valable pour tout  $x$  et tout  $y$  tels que  $s(x) = s(y)$ , nous en déduisons que  $s$  est injective. En d'autres termes, il existe une application injective de  $E$  vers  $F$ .

**Preuve (seulement si)** La preuve est de même nature.

## Cardinalité

La notion de cardinal s'étend à des ensembles infinis:

### Definition (Cardinal généralisé)

On dit que deux ensembles  $E$  et  $F$  ont le même cardinal s'il existe une bijection entre  $E$  et  $F$ .

On dit que le cardinal de  $E$  est au moins aussi grand que le cardinal de  $F$  s'il existe une injection de  $E$  vers  $F$ , ou encore s'il existe une surjection de  $F$  vers  $E$ .

### Théorème (Cantor Bernstein)

Considérons deux ensembles  $E$  et  $F$ . S'il existe une application injective de  $E$  vers  $F$  et une application surjective de  $E$  vers  $F$ , alors il existe une application bijective de  $E$  vers  $F$ .

### Pour réviser

Prouvez le théorème de Cantor Bernstein – ou, plus simplement, trouvez et comprenez une preuve de ce théorème.

## Vers la dénombrabilité

- Q Comparez le cardinal de  $\mathbf{N}$  et celui de  $\mathbf{N}^*$ .
- Q Comparez le cardinal de  $\mathbf{N}$  et celui de l'ensemble des entiers naturels pairs.
- Q Comparez le cardinal de  $\mathbf{N}$  et celui de  $\mathbf{N} \times \mathbf{N}$ .
- A Tous ces ensembles ont le même cardinal !

## Dénombrabilité

### Definition (Dénombrable)

Un ensemble  $E$  est *dénombrable* s'il existe une injection de  $E$  vers  $\mathbf{N}$ . Un ensemble  $E$  est *strictement dénombrable* s'il existe une bijection de  $E$  vers  $\mathbf{N}$ . On note alors le cardinal de  $E$   $\omega$ .

En d'autres termes, un ensemble est dénombrable si on peut numéroter ses éléments.

## Infini ?

### Definition (Infini)

Un ensemble  $E$  est dit *infini* s'il existe une injection de  $\mathbf{N}$  vers  $E$ .

### Théorème

Un ensemble  $E$  est dénombrable si et seulement si il est soit fini, soit strictement dénombrable.

### Devoir

Preuve ce théorème.

## Non-dénombrabilité ?

**Q** Existe-t-il des ensembles non dénombrable ?

**A** Oui. Par exemple  $\mathbf{R}$ .

### Exercice

Preuve que  $\mathbf{R}$  n'est pas dénombrable.

**Indice** Vous pourrez commencer par montrer que l'ensemble des suites à valeurs dans  $\{0, 1\}$  n'est pas dénombrable.



## Non-dénombrabilité !

### Lemme

L'ensemble  $\mathcal{U}$  des suites à valeurs dans  $\{0, 1\}$  n'est pas dénombrable.

Supposons le contraire. Il existe alors  $f : \mathcal{U} \rightarrow \mathbf{N}$  injective. Considérons alors l'application  $g = f^{-1}$ , qui sera surjective. Pour tout  $n$ ,  $g(n)$  est une suite à valeurs dans  $\{0, 1\}$ . Nous pouvons donc considérer la valeur  $g(n)_n$ , qui sera soit 0, soit 1.

Soit  $(u_n)_{n \in \mathbf{N}}$  la suite définie par "pour tout  $n$ ,  $u_n = 1 - g(n)_n$ ." Nous savons que

- ▶  $u_0 \neq g(0)_0$  donc  $u \neq g(0)$
- ▶  $u_1 \neq g(1)_1$  donc  $u \neq g(1)$
- ▶ ...
- ▶  $\forall i, u_i \neq g(i)_i$ ; donc  $u \neq g(i)$ .

Par conséquent,  $u$  n'est pas dans l'image de  $g$ . Ce qui contredit l'hypothèse.

Par l'absurde, nous venons de prouver que  $g$  n'est pas surjective, donc que  $f$  n'est pas injective, donc que  $\mathcal{U}$  n'est pas dénombrable.

## Et $\mathbf{R}$ ?

Pour prouver que  $\mathbf{R}$  n'est pas dénombrable, on raisonne de nouveau par l'absurde.

Si  $\mathbf{R}$  est dénombrable, alors  $[0, 1[$  aussi. Or il existe une injection de  $[0, 1[$  vers les suites à valeurs dans  $\{0, 1\}$  (l'écriture binaire du nombre – mais on pourrait se débrouiller en décimal, avec un lemme un tout petit peu plus compliqué). Par conséquent, si  $\mathbf{R}$  est dénombrable, l'ensemble des suites à valeurs dans  $\{0, 1\}$  est dénombrable. Comme nous venons de prouver que ceci est faux, nous pouvons en déduire que  $\mathbf{R}$  n'est pas dénombrable.



## Ensemble de parties

### Theorem

Soit  $E$  un ensemble. Il n'existe pas de bijection entre  $E$  et  $\mathcal{P}(E)$ .

**Preuve** Raisonnons par l'absurde et supposons l'existence d'une bijection  $f : E \rightarrow \mathcal{P}(E)$ .

Considérons la partie  $A$  de  $E$  définie comme  $\{a \in E / a \notin f(a)\}$ .

Comme  $f$  est surjective, il existe  $a$  dans  $E$  tel que  $f(a) = A$ .

Alors

- ▶ soit  $a \in A$ , auquel cas, par définition de  $A$ ,  $a \notin f(a)$ , c'est-à-dire  $a \notin A$ , ce qui est absurde
- ▶ soit  $a \notin A$ , auquel cas, par définition de  $A$ ,  $a \in f(a)$ , c'est-à-dire  $a \in A$ , ce qui est tout aussi absurde.

Par l'absurde, on en déduit que  $f$  n'est pas surjective, donc qu'il n'existe pas de bijection entre  $E$  et  $\mathcal{P}(E)$ .

Ce type de *raisonnement diagonal* est courant pour trouver des contre-exemples en mathématiques pour l'informatique.



## La frontière

**Q** Pourquoi différencier ainsi dénombrable et non-dénombrable ?

**A** Parce que, bien souvent, on ne sait raisonner que sur ce qui est dénombrable.

Un ensemble dénombrable a ceci de sympathique que

- ▶ on peut énumérer ses éléments
- ▶ on peut procéder à des récurrences !

Même dans les autres champs des mathématiques, les outils logiques restent dénombrables !



## Introduction

### Cardinalité

- Ensembles finis
- Ensembles dénombrables

### Relations

- Opérations
- Relations

## Conclusions



## Opérations

### Definition (Opérations)

Une *opération* sur un ensemble  $E$  est une application  $\Phi : E^n \rightarrow E$ . On appelle  $n$  l'*arité* de  $\Phi$ .

### Definition (Opérations binaires)

Une *opération binaire* (ou *loi de composition interne*) est une opération d'arité 2.

Si  $*$  est une opération binaire, on notera souvent  $x * y$  l'image du couple  $(x, y)$  par  $*$ .



## Propriétés classiques

### Definition (Associativité)

L'opération binaire  $*$  sur  $E$  est *associative* si, pour tout  $x, y, z$  dans  $E$ , on a  $x * (y * z) = (x * y) * z$ .

### Definition (Commutative)

L'opération binaire  $*$  sur  $E$  est *commutative* si, pour tout  $x, y$  dans  $E$ , on a  $x * y = y * x$ .

### Definition (Élément neutre)

Si  $*$  est une opération binaire sur  $E$  et si  $\mathbf{1}$  est un élément de  $E$ , alors  $*$  admet  $\mathbf{1}$  comme est *élément neutre* si, pour tout  $x$  dans  $E$ , on a  $x * \mathbf{1} = \mathbf{1} * x = x$ .



## Exemples

Q Dans  $\mathbf{N}$ , l'addition est-elle associative ? Commutative ? Admet-elle un élément neutre ?

Q Quid de la multiplication ? La soustraction ? La division ?

### Devoir (Unicité de l'élément neutre)

Si  $*$  est une opération binaire sur  $E$ , prouvez que  $*$  admet au plus un élément neutre.

## Vers les groupes

### Definition (Semi-groupe)

Un ensemble  $E$  muni d'une opération binaire associative  $*$  est appelé un *semi-groupe*.

### Definition (Monoïde)

Un semi-groupe muni d'un élément neutre  $e$  est appelé un *monoïde*.

### Definition (Monoïde libre)

Soit  $A$  un ensemble fini (*l'alphabet*). Le *monoïde libre* sur  $A$  est l'ensemble des suites finies de  $A$ . L'opération binaire est la concaténation  $\cdot$ . L'élément neutre est le mot vide  $\epsilon$ .



## Exemples

L'ensemble  $\mathbf{N}$ , muni de l'addition, est un monoïde.

L'ensemble des écritures de nombres est un monoïde libre sur  $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$  (on distingue 0, 00, 000...).



## Groupes

### Definition (Groupes)

Un *groupe* est un monoïde  $(E, *, \mathbf{1})$  dans lequel chaque élément admet un inverse. C'est-à-dire que pour tout  $e$  de  $E$ , il existe  $e'$  tel que  $e * e' = e' * e = \mathbf{1}$ .

Q Le monoïde  $(\mathbf{N}, +, 0)$  est-il un groupe ?

A Non : 1, par exemple, n'a pas d'inverse. Par contre,  $(\mathbf{Z}, +, 0)$  est un groupe.

## Relations

### Definition (Relation)

Si  $E$  est un ensemble, une *relation* sur  $E$  est un sous-ensemble de  $E \times E$ .

Si  $\mathcal{R}$  est une relation, pour signifier que  $x$  et  $y$  sont liés par  $\mathcal{R}$ , on notera au choix  $(x, y) \in \mathcal{R}$ ,  $\mathcal{R}(x, y)$  ou  $x\mathcal{R}y$ .

### Exemples

- ▶ L'égalité sur  $E$ , définie comme  $\{(x, x) / x \in E\}$ .
- ▶ L'infériorité sur  $\mathbf{N}$ .
- ▶ La divisibilité sur  $\mathbf{N}$ .
- ▶ L'adjacence géométrique.
- ▶ L'existence d'un chemin entre  $x$  et  $y$  dans un labyrinthe.

## Opérations sur les relations

### Definition (Inversion)

Si  $\mathcal{R}$  est une relation, la *relation inverse*  $\mathcal{R}^{-1}$  est définie par  $x\mathcal{R}^{-1}y \iff y\mathcal{R}x$ .

### Definition (Composition)

Si  $\mathcal{R}$  et  $\mathcal{R}'$  sont deux relations sur  $E$ , la *relation composée*  $\mathcal{R} \cdot \mathcal{R}'$  est la relation définie par  $x\mathcal{R} \cdot \mathcal{R}'y \iff \exists z / x\mathcal{R}z \wedge z\mathcal{R}'y$ .

### Definition (Clôture transitive)

Si  $\mathcal{R}$  est une relation sur  $E$ , sa *clôture transitive*  $\mathcal{R}^*$  est la relation définie par  $\mathcal{R}^* = \bigcup_{n \in \mathbf{N}} \mathcal{R}^n$ .

**Exemple** Si  $\rightarrow$  est la relation d'adjacence,  $\rightarrow^*$  est la relation d'existence de chemin.

## Propriétés des relations

### Definition

Soient  $E$  un ensemble et  $\mathcal{R}$  une relation. Alors  $\mathcal{R}$  sera dite

- réflexive** si,  $\forall e, e\mathcal{R}e$  ;
- symétrique** si,  $\forall e, f, e\mathcal{R}f \Rightarrow f\mathcal{R}e$  ;
- antisymétrique** si  $\forall e, f, e\mathcal{R}f \wedge f\mathcal{R}e \Rightarrow e = f$  ;
- transitive** si  $\forall e, f, g, e\mathcal{R}f \wedge f\mathcal{R}g \Rightarrow e\mathcal{R}g$

## Questions

Considérons la relation  $\mathcal{R}$  définie sur  $\mathbf{N}$  par  $m\mathcal{R}n \iff n = m + 1$ .

**Q** Cette relation est-elle réflexive ? Symétrique ? Antisymétrique ?

Transitive ? Quelle est sa clôture transitive ?

**Q** Quid de la relation  $\mathcal{R}$  définie sur  $\mathbf{N}$  par " $m\mathcal{R}n$  si et seulement si  $m$  et  $n$  ont au moins un diviseur commun autre que 1" ?

## Introduction

### Cardinalité

Ensembles finis

Ensembles dénombrables

### Relations

Opérations

Relations



## Conclusions



## Bilan

Nous avons introduit les notions de dénombrabilité et de relations. Ces notions sont omniprésentes en informatique, aussi bien que dans les autres branches des mathématiques.

## Pour la suite

Relations d'Équivalence, de Préordre, d'Ordre  
Treillis

