

Mathématiques pour l'Informatique

Vers l'infini

David Teller

2 mars 2009



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.

...

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 ?



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 .



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)

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



Propriété fondamentale

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 .



Lemme

Proposition ((Semi-)inverses)

Soit $f : E \rightarrow F$ une application.

- ▶ Si $E \neq \emptyset$, alors f est injective si et seulement si f a un inverse à gauche, c'est-à-dire s'il existe une application $r : F \rightarrow E$ telle que $r \circ f = Id_E$.
- ▶ f est surjective si et seulement si f a un inverse à droite, c'est-à-dire s'il existe une application $s : F \rightarrow E$ telle que $f \circ s = Id_F$.
- ▶ f est bijective si et seulement si f a un inverse, c'est-à-dire s'il existe une application $f^{-1} : F \rightarrow E$ telle que $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.

Exercice

Preuve cette proposition.



Preuve de la propriété

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 .

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 plus 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 .

Cantor Bernstein

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 .

Exercice

Trouvez dans la littérature et expliquez-moi 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 !

Exercice

Prouvez-le.

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 ω .

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.

Exercice

Prouvez ce théorème.



Non-dénombrabilité ?

Q Existe-t-il des ensembles non dénombrable ?

A Oui. Par exemple \mathbf{R} .

Exercice

Prouvez 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

Théorème

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

Exercice

Prouvez ceci.

Indice Pensez au barbier et au raisonnement diagonal.



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 !

