Cardinaux et dénombrabilité

Plan

- **Ensembles finis**
  - Cardinal d'un ensemble fini
  - Propriétés des ensembles finis
- **Ensembles infinis**
  - Généralisation de la notion d'ensemble infini et de cardinal
  - Dénombrabilité
  - Théorème de Cantor : Démonstration directe et argument diagonal
  - Théorème de Cantor : démonstration indirecte et justification de la nouvelle définition de l'infini

Ensembles finis (1)

PROBLEMATIQUE : intuitivement, le cardinal d'un ensemble fini E est son nombre d'éléments. Comment formaliser rigoureusement cette notion ?

Définition d'un ensemble fini / infini

E est *fini* s'il peut être mis en bijection avec un sous-ensemble de $\mathbb{N}$ de la forme {1 ;..; n} où $n \in \mathbb{N}$. On dit alors que E a pour cardinal n, et on note $|E| = n$

- Si tel n'est pas le cas, E est un ensemble *infini*

Exemples

- Soit E de cardinal m. Alors $\mathcal{P}(E)$ a pour cardinal 2^m
- Soit E de cardinal m et F de cardinal n. Alors l'ensemble des applications de E dans F a pour cardinal n^m
- L'ensemble des bijections de F vers lui-même a pour cardinal n!

Ensembles finis (2)

Propriétés des ensembles finis

- Soit E et F deux ensembles finis de même cardinal. Alors les propriétés suivantes sont équivalentes :
  1) f est injective
  2) f est surjective
  3) f est bijective
- Soient E et F deux ensembles finis disjoints
  Alors : $|E \cup F| = |E| + |F|$
- Soient E et F deux ensembles finis quelconques
  Alors : $|E \cup F| = |E| + |F| - |E \cap F|$
  Généralisation à n ensembles (formule du crible) :
  $|\cup_{1 \leq i \leq n} E_i| = \Sigma_{1 \leq k \leq n} (-1)^{k+1} \Sigma_{1 \leq i1 < i2 < \ldots < ik \leq n} |E_{i1} \cap \ldots \cap E_{ik}|$
- Soient E et F deux ensembles finis quelconques :
  Alors : $|E \times F| = |E| . |F|$
  Généralisation à n ensembles :
  $|E_1 \times E_2 \times \ldots \times E_n| = |E_1| . |E_2| . |E_n|$

Ensembles finis (3)

Propriétés des ensembles finis

- Il existe une injection de E dans F ssi I E I ≤ I FI
  Il existe une surjection de E dans F ssi I E I ≥ I FI
- Principe d'égalité :
  Il existe une bijection entre E et F ssi I E I = I F I
- Principe d'inégalité (ou principe des tiroirs) :
  Si I E I > I F I alors il n'existe pas d'injection de E dans F

  Ou de façon équivalente :

  s'il y a plus d'objets à ranger que de tiroirs, alors il existe au moins un tiroir qui contient plusieurs objets

Ensembles infinis (1)

PROBLEMATIQUE : peut-on "compter" le nombre d'éléments d'un ensemble infini ?

Définition fondamentale

Un ensemble est infini s'il peut être mis en bijection avec une de ses parties propres, sinon il est fini

- Exemples : ℕ vs ℕ*, ℕ vs 2ℕ, ℕ vs les carrés d'entiers,

Généralisation de la notion de cardinal

Deux ensembles quelconques E et F ont même cardinal (ou sont équipotents) s'il existe une bijection de E vers F. On note card(E) = card(F)

- Pour E et F finis, équipotence signifie "même nombre d'éléments"
- card(E) ≤ card(F) s'il existe une injection de E vers F
- Compatibilité avec le théorème de Cantor-Berstein

Ensembles infinis (2)

Définition de la dénombrabilité

Un ensemble infini est dénombrable s'il est équipotent à $\mathbb{N}$

Avantages pour l'informatique :

- ses éléments peuvent être numérotés
- on peut énumérer ses éléments

Conséquences

Sont dénombrables :

- ► Toute partie infinie de $\mathbb{N}$
- ► Tout ensemble infini qui peut être injecté dans $\mathbb{N}$
- ► Tout produit cartésien d'ensembles dénombrables

Exemples d'ensembles dénombrables

- ► $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{N}^2$, l'ensemble des carrés d'entiers
- ► Les ensembles des nombres premiers, algébriques,…
- ► L'ensemble des mots sur un alphabet fini

Ensembles infinis (3)

PROBLEMATIQUE : les ensembles infinis sont-ils tous dénombrables ? Une réponse décisive : NON

Théorème de Cantor

$\mathbb{R}$ n'est pas dénombrable !

Démonstration directe

Un grand classique : l'argument diagonal

Ensembles infinis (4)

Démonstration directe : illustration

x_1	0,	$\boxed{8}$	5	3	4	9	5	...
x_2	0,	2	$\boxed{6}$	0	1	7	3	...
x_3	0,	5	0	$\boxed{1}$	7	4	4	...
x_4	0,	2	7	6	$\boxed{4}$	5	4	...
x_5	0,	3	8	0	6	$\boxed{7}$	2	...
x_6	0,	9	1	3	6	5	$\boxed{8}$	...

$\rightarrow$ x = 0, 7 3 0 5 6 9 ....

Ensembles infinis (5)

Démonstration indirecte

Deux étapes :

Théorème 1

Quel que soit un ensemble E, il n'existe pas de bijection entre E et $\mathcal{P}$(E)

Conséquence : pour tout E, card(E) < card($\mathcal{P}$(E))

Théorème 2

$\mathbb{R}$ et $\mathcal{P}(\mathbb{N})$ sont équipotents

Conséquence

- $\mathbb{R}$ est indénombrable !!!
- Il existe une infinité d'infinis

Ensembles infinis (8)

Mesure de Lebesgue

S’applique aux ensembles de nombres

Notion de mesure d’un ensemble (simplifiée) : somme des longueurs des intervalles fermés

PROBLEMATIQUE : les ensembles infinis de mesure nulle (au sens de Lebesgue) sont-ils toujours dénombrables ?

Ensemble de Cantor

Ensemble remarquable : K3

Infini non dénombrable et de mesure nulle !

Ensembles infinis (9)

Une curiosité

Quelques propriétés “étranges” des ensembles dénombrables

L’hôtel de Hilbert

- Attribué à Hilbert (1862-1943)

  Un hôtel compte une infinité de chambres, toutes occupées :

  - *Peut-on accueillir un nouveau client ?*
  - *Un bus transportant une infinité de clients se présente à l’hôtel. Est-il possible de les accueillir tous ?*

Principes d'induction

:

Plan

- Principes de démonstration
- Principe d'induction général
- Principes de récurrence
  - Récurrence simple
  - Récurrence forte
  - Exemple curieux
- Induction vs Récursivité
- Définition inductive d'un ensemble

Principes de démonstration (rappels)

Pour démontrer une implication P ⇒ Q

- Méthode directe : on pose que P est vrai. On en déduit que Q est vrai
- Méthode par contraposition : parfois plus facile de démontrer non Q ⇒ non P

Pour démontrer une disjonction

Pour montrer que P ou Q est vrai :

- On montre que P est vrai ou que Q est vrai
- On montre que si l'un des deux est faux l'autre est vrai

Pour démonter une équivalence P ⇔ Q

- On montre P ⇒ Q et Q ⇒ P
- On procède par équivalences successives

Pour montrer P ⇔ Q ⇔ R : il suffit de montrer P ⇒ Q, Q ⇒ R et P ⇒ P

:

Principes de démonstration (rappels)

Raisonnement par l'absurde

On veut montrer P. On suppose P fausse ou non P vraie, et on aboutit à une contradiction

En particulier :

- ► Application à la démonstration de l'implication
- ► Pour démontrer qu'un ensemble est vide
- ► Pour démontrer l'unicité

Raisonnement par cas

Pour un raisonnement ou une démonstration comportant plusieurs cas (hypothèses) :

- Regrouper les cas en sous-ensembles homogènes
- S'assurer que les sous-ensembles sont disjoints 2 à 2
- Vérifier la réunion de tous les sous-ensembles n'élude aucun cas
- Raisonner, au sein de chaque groupe

Principe d'induction général

Preuves par induction bien fondée

Méthode de raisonnement qui vise à établir une propriété valable pour tous les éléments d'un ensemble

Le Principe Général d'Induction

Soit $(E,\preccurlyeq)$ un ensemble bien ordonné.

Soit P une propriété telle que :

- P est vraie pour tout élément minimal de E
- Pour tout élément non minimal x de E, si P est vraie pour tout $y < x$, alors P est vraie pour x.

Alors la propriété P est vraie pour tous les éléments de E.

:

Principe de récurrence

Premier principe d'induction sur $\mathbb{N}$

Récurrence faible

Soit P une propriété sur $\mathbb{N}$ tel que :

- P(0) soit vraie
- $\forall n \in \mathbb{N},\ P(n) \Rightarrow P(n+1)$

Alors pour tout n de $\mathbb{N}$, P(n) est vrai

Principes de récurrence

Autres principes d'induction sur $\mathbb{N}$, équivalents au premier

Récurrence forte ou généralisée

Soit P une propriété définie sur telle que $\mathbb{N}$:
- P(0) soit vraie
- $\forall n \in N$, $(\forall m < n \ P(m)) \Rightarrow P(n)$

Alors pour tout n de $\mathbb{N}$, P(n) est vérifiée

Démonstration : découle directement du principe général d'induction, $(\mathbb{N},\leq)$ étant bien ordonné

Récurrence d'ordre 2

Soit P une propriété définie sur telle que $\mathbb{N}$:
- P(0) soit vraie
- P(1) soit vraie
- $\forall n \in N$, $(P(n) \text{ et } P(n+1)) \Rightarrow P(n+2)$

Alors pour tout n de $\mathbb{N}$, P(n) est vérifiée

:

Définitions inductives

Définitions inductives (ou *récursives*) abondamment utilisées en Informatique

Généralités

Notions informatiques :
- Ensembles
- Structures de données : expressions arithmétiques, arbres
- Programmes

Deux étapes principales :
- ► Donnée explicite de quelques éléments d'un ensemble infini (la base)
- ► Donnée d'un procédé qui permet de définir les autres éléments à partir de ceux qui y sont déjà

Avantage principal : utilisation des principes d'induction pour démontrer des propriétés sur des ensembles ainsi définis

Induction et Ensembles

Troisième façon de définir un ensemble

Définition inductive d'un ensemble

Soit E un ensemble préalablement défini, et X un ensemble de base inclus dans E

Un ensemble G est défini inductivement (récursivement) si :

1. $X \subset G$
2. des règles d'induction $f : E^n \rightarrow F$
   si $x_1,\ldots,x_n \in G$ alors $f(x_1,\ldots,x_n) \in G$
3. un principe de minimalité : G est le plus petit ensemble qui vérifie les deux conditions précédentes

Exemple

Construction de $\mathbb{N}$ (extrêmement simplifiée) :

- $0 \in \mathbb{N}$
- si $n \in \mathbb{N}$ alors $n+1 \in \mathbb{N}$

: