Notions d'ensembles et dénombrabilité

2ème séance du cours "Introduction à l'Informatique Théorique" – Master Systèmes Complexes

Disclaimer. Deux explications avant de commencer.

1. Ces notes seront plutôt décharnées et probablement trop techniques. Il s'agit d'une stratégie interactive : si vous voulez qu'une partie, une notation, des intuitions ou un résultat soit mieux expliqué, faites-le savoir et je vous contenterai !
2. Vous allez certainement trouver des fautes, soit de langue soit de contenu (j'espère moins). N'hesitez surtout pas à me les signaler !

1 Un peu de notations

Un ensemble est intuitivement un groupe d'objets vu comme une unité. C'est une collection d'objets ou on compte pas ni l'ordre ni les répétitions.

Les lettres majuscules de l'alphabet (A, B, S,...) seront en général utilisés comme des variables d'ensembles.

Les accolades { et } sont presque universellement utilisé pour dénoter des ensemble, comme dans les exemples suivantes.

1. Ensemble présenté par une liste exhaustive : $\{ 3, 5, \infty, \perp \}$;
2. ensemble présenté par une liste à compléter : $\{ 2, 4, 6, \dots \}$, $\{ 1, 2, \dots, 100 \}$;
3. ensemble présenté par une propriété : $\{ x \in \mathbb{N} \mid \exists k \in \mathbb{N}, x = 2k \}$ ou plus brièvement $\{ 2k \mid k \in \mathbb{N} \}$, $\{ p \in \mathbb{N} \mid p \text{ est premier} \}$.

$\mathbb{N}$ ci-dessus est l'ensemble des naturels $\{ 0, 1, 2, 3, \dots \}$. Autres ensembles de nombres qu'on verra :

1. $\mathbb{Z}$: les entiers $\{ \dots, -2, -1, 0, 1, 2, \dots \}$;
2. $\mathbb{Q}$: les rationnels $\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}, n \neq 0 \}$;
3. $\mathbb{R}$: les réels.

Voici des notations qu'on va utiliser pour les opérations plus communes sur les ensembles.

- $a \in A$ (et son contraire $a \notin A$) : "a appartient à S".
- $A \subseteq B$ (et son contraire $a \not\subseteq A$) : "A est un sous-ensemble de B, c.-à-d. $\forall a \in A : a \in B$. Notez que $A = B$ ssi[1] $A \subseteq B$ et $B \subseteq A$.

1. "ssi" est un raccourci pour "si et seulement si".

- $A \subsetneq B$: A est un sous-ensemble propre de B, c.-à-d. $A \subseteq B$ et $A \neq B$, c.-à-d. $A \subseteq B$ et $\exists b \in B : b \notin A$.
- $A \cup B$, $A \cap B$ et $A \setminus B$: respectivement union, intersection et soustraction ($A \setminus B = \{ x \in A \mid x \notin B \}$).
- $\mathcal{P}(A)$: l'**ensemble des parties** de A, c.-à-d. $\mathcal{P}(A) = \{ S \subseteq A \}$.
- $A \times B$: le produit cartésien de A et B, c.-à-d. l'ensemble de couples $\{ (a, b) \mid a \in A, b \in B \}$.
- A^n : l'ensemble des n-uples $(x_1, \ldots, x_n)$ à éléments dans A ; on pose $A^0 = \{ () \}$ l'ensemble avec un seule élément noté () (l'n-uplet vide). S'il y a pas de confusion, on peut aussi bien noter $(x_1, \ldots, x_n)$ par $x_1 \cdots x_n$, (un **mot** a n caractères dans A), et () par ε (le **mot vide**).
- A^B : l'**espace des fonctions** de B a A, c.-à-d. $A^B = \{ f : B \to A \}$. Pour exemple, $A^{\mathbb{N}}$ est l'espace des fonctions de $\mathbb{N}$ à A, qu'on appelle habituellement **suites** à valeurs dans A. On peut aussi bien noter les suites dans $A^{\mathbb{N}}$ par des n-uplets infinies $(x_0, x_1, x_2, \ldots)$. La composition des fonction $f : A \to B$ et $g : B \to C$ est noté par $g \circ f$. Pour chaque $S \subseteq A$ on notera avec $f(S) \subseteq B$ l'**image de S à travers** f, c.-à-d. $f(S) = \{ f(a) \mid a \in S \}$.

> *Le paradoxe de Russel.* Dans la première présentation d'une rigoureuse théorie mathématique des ensembles due à Georg Cantor il figurait la possibilité de *toujours* construire un ensemble à partir d'une propriété quelconque. Étant donnée une propriété $P(x)$, on aurait donc toujours l'ensemble $\{ x \mid P(x) \}$. Cette idée *a priori* intuitive emmène en fait à un paradoxe découvert par Russel.
>
> L'idée se de prendre comme propriété celle de "ne pas contenir soi-même comme élément", ou en symboles $x \notin x$. Alors si on note $S = \{ x \mid x \notin x \}$, on verra que
>
> $$S \in S \iff S \notin S$$
>
> qui est une contradiction !
>
> On peut dire que le paradoxe de Russel est une variation du célèbre paradoxe du philosophe crétois Épiménide, qui avait déclaré que "tous les crétois sont des menteurs". La théorie des ensembles de Cantor est aujourd'hui appelée théorie *naïve* des ensembles.
>
> Dans la théorie moderne (due à Zermelo et Fraenkel) le paradoxe est évité en limitant la création d'un ensemble A à partir d'une propriété P que quand on sait déjà qu'il existe un ensemble B dans le quel on choisit les éléments de A. Une des conséquences est qu'il peut pas exister un ensemble de tous les ensembles... En tout cas il faut pas s'effrayer, on va jamais tomber sur ces problèmes : chaque fois qu'on écrira un ensemble par une propriété, on sera sur un côté "sur" de la théorie.

On rappelle ici les définitions d'injectivité, surjectivité et bijectivité.

- $f : A \to B$ est **injective** si $f(a) = f(a')$ implique $a = a'$.
- $f : A \to B$ est **surjective** si pour tous $b \in B$ il existe $a \in A$.
- $f : A \to B$ est **bijective** (noté $f : A \leftrightarrow B$) si elle est injective et surjective.

Remarque 1. Soit $f : A \to B$.

- f est injective ssi il existe $g : B \to A$ t.q. $\forall a \in A : g(f(a)) = a$ (inverse gauche).
- f est surjective ssi il existe $g : B \to A$ t.q. $\forall b \in B : f(g(b)) = b$ (inverse droite).
- f est bijective ssi il existe $f^{-1} : B \to A$ t.q. $f^{-1}(f(a)) = a$ et $f(f^{-1}(b)) = b$ pour tous a et b.

Preuve.

- Si f est injective, soit a_0 un élément quelconque de A, et définissons $g : B \to A$ par

$$g(b) = \begin{cases} a & \text{si } b = f(a) \text{ (c.-à-d. } b \in f(A)), \\ a_0 & \text{sinon.} \end{cases}$$

  Il y a pas d'ambiguité dans la définition : on ne peut pas avoir deux a, a' différents avec $f(a) = b = f(a')$. Pour cette raison on va avoir $g(f(a)) = a$ par définition de g.
  Pour l'autre direction, s'il y a g t.q. on a toujours $g(f(a)) = a$ alors si $f(a) = f(a')$ on peut appliquer g sur les deux côtés et obtenir $a = g(f(a)) = g(f(a')) = a'$.
- Si f est surjective, alors il suffit de définir g en prennent pour chaque $b \in B$ l'élément de A dont l'existence est assuré par la définition de surjectivité. *Vice versa* il suffira d'utiliser $g(b)$ pour voire que la définition de surjectivité est satisfaite.
- Par les deux points précédents si f est bijective alors ils existent $g, g' : B \to A$ avec $g(f(a)) = a$ et $f(g'(b)) = b$ pour tous $a \in A$, $b \in B$. Or pour tous b on a

$$g(b) = g(f(g'(b))) = g'(b),$$

  donc $g = g' = f^{-1}$. L'autre direction est immédiate.

Remarque 2. Pour tous ensemble A il existe la bjection $\delta : \mathcal{P}(A) \leftrightarrow \{0,1\}^A$. Pour chaque $S \subseteq A$ il faut definir une fonction $\delta(S) : A \to \{0,1\}$ (qu'on va noter δ_S pour ne pas gâcher de parenthèses...). Alors

$$\delta_S(x) = \begin{cases} 1 & \text{si } x \in S, \\ 0 & \text{sinon} \end{cases}$$

(appelée la **fonction caractéristique** de S) est la fonction souhaitée.

2 La taille des ensemble : la cardinalité

Si un ensemble est fini, sa **cardinalité** est rien d'autre que le nombre de ses éléments, et elle est noté par $\#\{a_1, \ldots, a_k\} = k$. Le seul ensemble avec cardinalité 0 est l'**ensemble vide** noté par $\emptyset$.

Mais peut-on "compter" un ensemble s'il est infini ? Dans ce cas on peut plutôt comparer deux ensembles et dire (même si les deux ont une infinité d'éléments) qu'ils ont le "même nombre d'éléments". Comment ? Il suffit de trouver un bijection entre le deux.

Définition 3. On dit que deux ensemble A et B ont la **même cardinalité** (noté $\#A = \#B$) s'il existe une bijection $\phi : A \leftrightarrow B$.

Exemple 4. On va voire que $\#\{\,2k \mid k \in \mathbb{N}\,\} = \#\mathbb{N}$.

On définit tout simplement $\phi : \{\,2k \mid k \in \mathbb{N}\,\}$ par $\phi(2k) = k$, et on remarque qu'il s'agit bien d'une bijection.

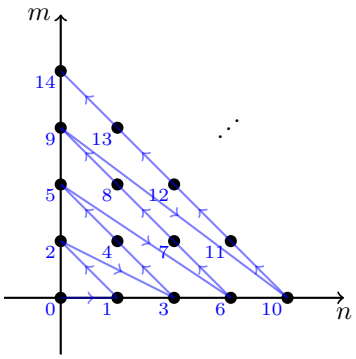
On peut noter par l'exemple ci-dessus qu'il peut bien arriver qu'un ensemble aie la même cardinalité d'un de ses sous-ensembles propres. En effet c'est une propriété qui caractérise les ensembles infinis !

Le grand hôtel d'Hilbert. Cet aspect apparemment contrintuitif de l'infini a été bien expliqué par Hilber. Vous pouvez en savoir plus sur `http://en.wikipedia.org/wiki/Hilbert's_paradox_of_the_Grand_Hotel`.

Exemple 5. On va maintenant voire que $\#\mathbb{N} \times \mathbb{N} = \#\mathbb{N}$. À ce but on peut utiliser la fonction $\beta : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ introduite par Cantor, definie par

$$\beta(n, m) = \frac{(n+m)(n+m+1)}{2} + m.$$

Graphiquement il s'agit de parcourir le treillis comme montré ici :



Preuve. Montrons que β est bijective.

Injectivité. Supposons $\beta(n, m) = \beta(n', m')$ et définissons $s = n + m$ et $t = n' + m'$. Si on prouve que $s = t$ alors on en tire que

$$m = \beta(n, m) - \frac{s(s+1)}{2} = \beta(n', m') - \frac{t(t+1)}{2} = m'$$

et puis que $n = n'$ aussi.
Supposons donc que $s \neq t$, et sans perte de généralité que $s < t$ (ou $s + 1 \leq t$). Grace à la formule $\frac{s(s+1)}{2} = \sum_{i=1}^{s} i$ et au fait que $m \leq s$ et

$m' \geq 0$ on peut voire que

$$\beta(n,m) = \sum_{i=1}^{s} i + m < \sum_{i=1}^{s} i + s + 1 = \sum_{i=1}^{s+1} i = \frac{s+1}{s+2} 2 \leq \frac{t(t+1)}{2} + m' = \beta(n',m')$$

donc que $\beta(n,m) \neq \beta(n',m')$ qui constitue une contradiction. Donc $s = t$ et on a prouvé l'injectivité.

Surjectivité. On va à nouveau se servire de la formule $\sum_{i=1}^{s} i = \frac{s(s+1)}{2}$. Étant donné $k \in \mathbb{N}$, soit

$$s = \max \left\{ t \mid \frac{t(t+1)}{2} \leq n \right\},$$

on va voire que $m = n - \frac{s(s+1)}{2}$ et $n = s - m$ sont tels que $\beta(n,m) = k$. Que la formule donnée par β soit valide est facilement vérifiable. Ce qui manque à savoir est si $n, m \in \mathbb{N}$, c.-à-d. s'ils sont positifs. Cela se réduit à vérifier que $0 \leq m = k - \frac{s(s+1)}{2} \leq s$.
Le fait que $0 \leq m$ vient directement de la définition de s, parce que $\frac{s(s+1)}{2} \leq k$. En raisonnant par absurde supposons donc que $m > s$ ou bien $m \geq s + 1$, c.-à-d.

$$k \geq \frac{s(s+1)}{2} + s + 1 = \sum_{i=1}^{s} i + s + 1 = \sum_{i=1}^{s+1} i = \frac{(s+1)(s+2)}{2}.$$

Cela contredit la définition de s car $s + 1$ est plus grand et a encore la propriété qui le caractérise.

Exercice 6. Soit $\psi : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ définie par $\psi(n,m) = 2^n(2m+1) - 1$. Prouver que ψ est bien une bijection.
Suggestion. Pour l'injectivité, supposer par absurde que pour $\phi(n,m) = \phi(n',m')$ on a $n < n' \ldots$

On se peut demander si tous les ensembles infinies on en fait la même cardinalité. On trouve que non grâce au résultat suivant dû à Cantor.

Théorème 7. *Aucune $f : A \to \mathcal{P}(A)$ ne peut être surjective, et donc $\# A \neq \# \mathcal{P}(A)$.*

Pour montrer ce théorème on utilise une procédure dite de *diagonalisation*, qui a une grande importance en logique et informatique théorique pour montrer des résultats négatifs comme celui ci-dessus.

Preuve. On procède par absurde, en supposant qu'il existe une telle $f : A \to \mathcal{P}(A)$. Pour plus de clarté prenons $\{0,1\}^A$ au place de A (on peut le faire grâce à ce qu'on a vu avec le Remarque 2).

Supposons donc que pour toutes $\delta : A \to \{0,1\}$ on a $a \in A$ avec $f(a) = \delta$. On souhaite construire $\epsilon : A \to \{0,1\}$ qui le contredit : il suffit que pour tous $a \in A$ il y aie au moins un $b \in A$ t.q. $\epsilon(b) \neq f(a)(b)$.
On va alors prendre $\epsilon(a) = 1 - f(a)(a)$ (dont on parle de diagonale) : en effet pour chaque a c'est exactement sur a qu'on est sûr d'avoir une valeur différente, car $f(a)(a) \neq 1 - f(a)(a) = \epsilon(a)$. On a trouvé une fonction $A \to \{0,1\}$ qui n'est pas l'image d'un a à travers f, ce qui contredit la surjectivité de f.

Définition 8. À part voire si deux ensembles ont la même taille, on pourrait se demander si un est plus grand que l'autre. On définie que A a une cardinalité inférieure à celle de B (écrit $\# A \leq \# B$) s'il existe une injection $\phi : A \to B$.

Exemple 9. On a vu que forcement $\# A \neq \# \mathcal{P}(A)$. On peut en fait voire que $\# A < \# \mathcal{P}(A)$ car $\phi(a) = \{a\}$ (le **singleton** contenant a) est une injection de A dans $\mathcal{P}(A)$.

Le théorème suivant permet de dire qu'en effet si A est plus grand B et *vice versa*, il veut dire qu'ils ont la même taille. Même si très intuitif, ce n'est pas immédiat, car il faut tirer une bijection à partir de deux injections qui *a priori* n'ont rien à voire l'une avec l'autre.

Théorème 10 (Cantor-Bernstein)**.** *Si* $\# A \leq \# B$ *et* $\# B \leq \# A$ *alors* $\# A = \# B$.

Preuve.* Par hypothèse, on a $f : A \to B$ et $g : B \to A$ injectives. On va produire une bijection $h : A \leftrightarrow g(B)$, qui composée avec $g^{-1} : g(B) \leftrightarrow B$ donnera la bijection souhaitée $g^{-1} \circ h : A \leftrightarrow B$.
Considerons la famille A_i des sousensembles de A definies récursivement par

$$\begin{aligned} A_0 &:= A \setminus g(B), \\ A_{k+1} &:= g(f(A_k)), \end{aligned}$$

et définissons

$$h(a) := \begin{cases} g(f(a)) & \text{si } a \in \bigcup_{i=0}^{\infty} A_i, \\ a & \text{sinon.} \end{cases}$$

Pour voir que $h(a) \in g(B)$, notez que si $a \notin \bigcup_{i=0}^{\infty} A_i$ en particulier $a \notin A_0 = A \setminus g(B)$, donc forcemment $a \in g(B)$.

Injectivité de h. Supposons $h(a) = h(b)$. Il y aurait trois cas : soit a et b son les deux dans $\bigcup_{i=0}^{\infty} A_i$, soit les deux ne le sont pas, soit un (p.ex. a) l'est et l'autre ne l'est pas.
- $a, b \in \bigcup_i A_i$: alors $g(f(a)) = g(f(b))$ et par injectivité des deux fonctions on a $a = b$;
- $a, b \notin \bigcup_i A_i$: par définition $a = b$;
- $a \in \bigcup_i A_i \not\ni b$: par définition on a $g(f(a)) = b$ et $a \in A_k$ pour un k ; mais alors $b \in A_{k+1} \subseteq \bigcup_{i=0}^{\infty}$ donc en effet ce cas ne se produit jamais.

Surjectivité de h. Soit $a = g(b) \in g(A)$ (qui entraine $a \notin A_0$). Si $a \notin \bigcup_{i=0}^{\infty}$ alors on a $a = h(a)$. Si d'autre part $a \in \bigcup_{i=0}^{\infty}$ alors il existe k t.q. $a \in A_{k+1} = g(f(A_k))$, c.-à-d. $a = f(g(a'))$ avec $a' \in A_k$, donc $a = h(a')$.

Exercice 11. Montrer que $\#\,\mathbb{Z} = \#\,\mathbb{Q} = \#\,\mathbb{N}$.

Exemple 12. On a que $\#\,\mathbb{N} < \#\,\mathbb{R}$. L'injection est en fait directe du fait que $\mathbb{N} \subseteq \mathbb{R}$. Puis on montre que $\{0,1\}^{\mathbb{N}} \leq \#\,\mathbb{R}$, et donc on obtient la chaîne

$$\#\,N < \{0,1\}^{\mathbb{N}} \leq \#\,\mathbb{R}.$$

Pour l'injection il suffit d'envoyer une fonction caractéristique δ dans l'expansion décimale $\phi(\delta) = 0, \delta(0)\delta(1)\delta(2)\cdots$.

Définition 13. On dit qu'un ensemble A est **dénombrable** si $\#\,A \leq \#\,\mathbb{N}$.

Exercice 14. Montrer que si A et B sont dénombrables, alors $A \cap B$, $A \cup B$ et $A \times B$ le sont aussi.