Combinatoire, Probabilités, Statistiques

Adrian TANASĂ

CM 2

Combinatoire

- En **combinatoire énumérative**, on va définir des ensembles d'objets d'intérêt, et chercher à les *énumérer* : dire combien ils ont d'éléments (souvent, il y aura des paramètres).
- En **combinatoire bijective**, on va chercher à “expliquer” des égalités du type $\#A = \#B$ (les ensembles A et B ont le même nombre d'éléments) par la description d'une *bijection* (la plus simple possible) entre A et B.
- Pour cela, on a besoin d'être capable d'interpréter certains cardinaux comme décrivant “naturellement” certains ensembles, et certaines opérations sur les cardinaux comme correspondant à des “opérations” sur les ensembles.
- Les objets seront souvent des mots, des arbres, des chemins. . .

Deux principes fondamentaux

A, B désignent des ensembles *finis*.

- **Principe additif :** si A et B sont deux ensembles **disjoints**, alors
$$\#(A \cup B) = \#A + \#B.$$
- **Principe multiplicatif :** quelques soient les ensembles finis A et B, on a
$$\#(A \times B) = \#A \cdot \#B.$$

Version moins abstraite

J'ai un ensemble d'objets C, décrit de manière complexe à partir des objets de deux ensembles A et B, et je veux savoir combien C contient d'objets.

- **Codage :** si j'arrive à établir une bijection entre mon ensemble C et un ensemble A (codage bijectif : chaque objet $c \in C$ est codé par un unique objet $a \in A$, et chaque objet $a \in A$ code un unique objet $c \in C$), alors $\#C = \#A$.
- **Principe additif :** si chaque objet de C est (codé par) soit un objet de A, soit un objet de B (et jamais les deux à la fois), alors le cardinal et C est le cardinal de A plus le cardinal de B.
- **Principe multiplicatif :** si chaque objet de C est (codé par) la donnée d'un objet de A et d'un objet de B (sans conditions), alors le cardinal de C est le cardinal de A multiplié par le cardinal de B.

Conséquences faciles

En itérant les deux principes (additif et multiplicatif), on en obtient des versions à n'importe quel nombre d'ensembles :

- pour n'importe quel n, si les n ensembles $A_1, \ldots, A_n$ sont **deux à deux disjoints**, alors

$$\#\left(\bigcup_{i=1}^{n} A_n\right) = \sum_{i=1}^{n} \#A_i.$$

- pour n'importe quel n,

$$\#\left(A_1 \times A_2 \times \cdots \times A_n\right) = \prod_{i=1}^{n} \#A_i.$$

- en particulier, $\#(A^n) = (\#A)^n$

(Preuves : par récurrence sur n)

Cardinal d'une union, en général

On a une formule plus générale que le principe additif, valable quelques soient les ensembles :

Théorème

Soient A et B deux ensembles finis quelconques. On a

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

En particulier, on a toujours $\#(A \cup B) \leq \#A + \#B$.

Preuve : On commence par écrire $A \cup B$ comme union de trois ensembles deux à deux distincts :
$A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$.
Puis, on remarque que A est l'union de deux d'entre eux :
$A = (A - B) \cup (A \cap B)$; et de manière similaire pour B :
$B = (B - A) \cup (A \cap B)$.
On écrit le principe additif pour chaque union, on triture, et...
Conséquence (évidente ?) : Si $A \subset B$, alors $\#A \leq \#B$.

Fonctions

Soit E et F deux ensembles et
f une fonction de E vers F ($f : E \to F$)

- si $x \in E$, $f(x) \in F$ est son **image** par f ;
  si $f(x) = y$, x est un **antécédent** par f
  (*Remarque* : il peut *a priori* y en avoir plus d'un).
- **Notations :** si $A \subset E$, $f(A) = \{y \in F : \exists x \in A, y = f(x)\}$
  (image de l'ensemble A par F) ; si $B \subset F$,
  $f^{-1}(B) = \{x \in E : f(x) \in B\}$ ("image réciproque" ou
  "préimage" de l'ensemble B par f)
- f est **surjective** (une surjection) si chaque $y \in F$ a au moins un antécédent.
- f est **injective** (une injection) si chaque $y \in F$ a au plus un antécédent ; autrement dit, si $f(x) = f(x')$, alors $x = x'$.
- f est **bijective** (une bijection) si elle est à la fois injective et surjective ; autrement dit, chaque $y \in F$ a **exactement** un antécédent.
  (Une bijection entre deux ensembles établit une correspondance exacte entre leurs éléments)

Bijections et cardinaux

L'existence d'injections ou de surjections entre E et F se traduit sur la finitude des ensembles, et sur leurs cardinaux :

- S'il existe une surjection de E vers F, et que E est fini, alors F est fini, et $\#E \geq \#F$.
- S'il existe une injection de E vers F, et que F est fini, alors E est fini, et $\#E \leq \#F$.
- Par conséquent, s'il existe une bijection de E vers F, et que l'un des deux ensembles est fini, alors l'autre l'est également, et $\#E = \#F$.
- Réciproquement : si $\#E = \#F$, alors il existe une bijection de E vers F.
- Injections et ensembles finis :
  si E et F sont deux ensembles **finis**, avec $\#E = \#F$, et que f est une injection de E vers F, alors f est forcément une bijection.

Réciproque d'une bijection

E et F deux ensembles ; on suppose que f est une bijection de E vers F.

- On peut définir une fonction $g : F \to E$ de la manière suivante : pour tout $y \in F$, il existe un unique $x \in E$ tel que $f(x) = y$ (puisque f est une bijection) ; on pose

$$g(y) = x$$

- Cette fonction g est appelée **réciproque** de f, aussi notée f^{-1} ; c'est une bijection de F vers E.
- On a systématiquement :
  - pour tout $x \in E$, $g(f(x)) = x$
  - pour tout $y \in F$, $f(g(y)) = y$
- **Intuitivement :** si f est une fonction de *codage* pour des objets, f^{-1} est la fonction de *décodage* correspondante.

Séquences et mots

- $A \times B$ est l'ensemble des **couples** formés d'un élément de A, puis d'un élément de B : $A \times B = \{(a, b) : a \in A, b \in B\}$ (dans un couple, "l'ordre compte" : $(a, b) \neq (b, a)$ si $a \neq b$)
- Pour $A = B$, on note aussi A^2 pour $A \times A$.
- Les couples d'éléments de A sont aussi, en fait, les **suites de longueur 2** d'éléments de A.
- Plus généralement, A^n (pour un entier $n > 0$) est l'ensemble des **séquences (ou suites) de longueur n, d'éléments de** A.
- Au lieu de **séquences**, on peut aussi parler de **mots** : en considérant A comme un "alphabet" dont les éléments sont appelés "lettres", on appelle également "mots de longueur n sur l'alphabet A" les éléments de A^n. Par convention, A^0 contient un unique élément, noté ε ("le mot vide").
- **Notations sur les mots :** $|w|$ pour la longueur du mot w ; w_i pour la i-ème lettre de w $(1 \leq i \leq |w|)$; et si a est une lettre, $|w|_a$ pour le *nombre d'occurrences de a dans w*, soit $|w|_a = \#\{i \in [[1, |w|]] : w_i = a\}$

Mots (suite)

- On introduit la notation A^*, correspondant à la définition

$$A^* = \bigcup_{n \in \mathbb{N}} A^n.$$

(ensemble de **toutes** les suites finies d'éléments de A)

- Sur les mots, on a une nouvelle opération : la **concaténation** : si $w \in A^n$ et $w' \in A^m$, $w \cdot w' \in A^{n+m}$ est défini ainsi : $w \cdot w'$ est le mot w'' défini par

$$w''_i = \begin{cases} w_i & \text{si } 1 \leq i \leq n \\ w'_{i-n} & \text{si } n+1 \leq i \leq n+m \end{cases}$$

- On note souvent les mots sans parenthèses quand cela ne prête pas à confusion : (a, a, b) devient aab ; ainsi, on a $abba \cdot abc = abbaabc$.

Classe combinatoire

En combinatoire, on va souvent chercher à “compter les objets d’un certain type”.

Le plus souvent, l’ensemble de tous les objets en question est infini, donc la réponse est en apparence simple : “il y en a une infinité”.

Mais on a généralement une notion de taille des objets, et la vraie question est plutôt : “combien y a-t-il d’objets de taille n, exprimé comme une fonction de n ?”

Classe combinatoire - définition

Définition :

Une classe combinatoire est la donnée d'un ensemble C, et d'une fonction

$$t : C \to N,$$

t. q. pour tout n, l'ensemble C_n des éléments de C qui ont n pour image par t est fini.

$$C_n = \{x \in C \mid t(x) = n\}.$$

La suite de comptage de la classe C est alors simplement la suite $(cn)_{n\geq 0}$ définie par : pour tout n, $c_n = \# C_n$.

La fonction t est appelée fonction de taille pour la classe ; si on change t, on change généralement de suite de comptage (et même, on peut ne plus avoir une classe combinatoire).

Un exemple

On prend un alphabet à 2 lettres, $A = \{a, b\}$, et comme ensemble, $C = A^*$: tous les mots sur l'alphabet A.

- avec comme fonction taille, la longueur du mot, $t(w) = |w|$: on a une classe combinatoire, et la suite de comptage est $a_n = 2^n$ (car $C_n = A^n$: on a une formule directe) ;
- avec comme fonction taille, le nombre d'occurrences de la lettre a ($t'(w) = |w|_a$), on n'a pas une classe combinatoire : en effet on peut former une infinité de mots de "taille" 0 (mots sans la lettre a : b, bb, $bbb \ldots$).

Les principes fondamentaux : version comptage

- **Principe additif :** si on peut assimiler les objets d'une classe C, soit aux objets de la classe A, soit aux objets de la classe B (mais jamais les deux à la fois), alors on peut écrire une égalité sur les suites de comptage :

$$c_n = a_n + b_n$$

- **Principe multiplicatif :** si, pour décrire un élément de notre ensemble, on peut le faire avec une séquence de choix :
  - d'abord un choix parmi n choix
  - puis, quelque soit le premier choix, on a toujours m choix

  alors le nombre d'éléments de notre ensemble est $n \cdots m$ (car la description des "choix" donne une bijection avec $[[1, n]] \times [[1, m]]$
- (et les généralisations à des sommes de plus de termes, ou produits de plus de facteurs)

Comptage direct d'une classe combinatoire

Réaliser le comptage d'une classe combinatoire, c'est en règle générale trouver une formule pour sa suite de comptage.
La méthode "directe" pour cela, c'est de trouver un *codage* pour les objets d'une taille n fixée : décrire une façon *exhaustive* et *non ambigüe* de définir un objet de taille n, de manière à ce qu'on soit capable d'écrire une formule pour le nombre de codages.

- **exhaustive :** chaque objet doit avoir un codage
- **non ambigüe :** chaque objet ne doit avoir qu'un seul codage

Parfois, on n'obtient pas une formule pour la suite, mais seulement une **relation de récurrence** qui permet de calculer facilement les termes de la suite de proche en proche, mais qu'on ne sait pas résoudre en une formule close.

Comptage direct d'une classe combinatoire

Réaliser le comptage d'une classe combinatoire, c'est en règle générale trouver une formule pour sa suite de comptage.
La méthode "directe" pour cela, c'est de trouver un *codage* pour les objets d'une taille n fixée : décrire une façon *exhaustive* et *non ambigüe* de définir un objet de taille n, de manière à ce qu'on soit capable d'écrire une formule pour le nombre de codages.

- **exhaustive :** chaque objet doit avoir un codage
- **non ambigüe :** chaque objet ne doit avoir qu'un seul codage

Parfois, on n'obtient pas une formule pour la suite, mais seulement une **relation de récurrence** qui permet de calculer facilement les termes de la suite de proche en proche, mais qu'on ne sait pas résoudre en une formule close.