COMBINATOIRE ET PROBABILITÉS DISCRÈTES

Chapitre 1 : Dénombrements élémentaires

Notation : $\forall p, q \in \mathbb{N}, [\![p, q]\!] = [p, q] \cap \mathbb{N}$.

I. Cardinal d'un ensemble

Propriété : soit $n \in \mathbb{N}$; il n'existe pas de bijection de $[\![1, n]\!]$ sur l'une de ses parties propres.

Définition : deux ensembles E et F ont *même cardinal* s'il existe une bijection de E sur F ; E est dit *fini de cardinal* $n \in \mathbb{N}$ s'il a même cardinal que $[\![1, n]\!]$; E est dit *dénombrable* s'il a même cardinal que $\mathbb{N}$, et *au plus dénombrable* s'il est fini ou dénombrable.

Notation : le cardinal de E est noté $|E|$, ou $\#E$, ou encore $\mathrm{Card}E$.

Propriétés : $\mathrm{Card}\emptyset = 0$; si E est fini et $A \subset E$, alors A est fini et $|A| \leqslant |E|$.

Proposition : E est fini ssi E ne peut être mis en bijection avec aucune de ses parties propres.

Dans la suite, tous les ensembles sont finis

II. Première constructions

Propriété : $E \cap F = \emptyset \implies |E \cup F| = |E| + |F|$.

Notation : si $E \cap F = \emptyset$, leur union *disjointe* est notée $E \sqcup F$.

Propriété : Plus généralement, $\left|\bigsqcup_{i \in I} A_i\right| = \sum_{i \in I} |A_i|$

Définition : on appelle *partition d'un ensemble* E tout ensemble de parties disjointes de E dont l'union (disjointe) est égale à E.

Propriétés : si $A \subset E$, $|E \setminus A| = |E| - |A|$; $\quad |E \cup F| + |E \cap F| = |E| + |F|$;
$|E \times F| = |E| \cdot |F|$, et plus généralement, $\left|\prod_{i \in I} A_i\right| = \prod_{i \in I} |A_i|$. En particulier, $|A^n| = |A|^n$.

III. Applications et sous-ensembles

Notation : F^E désigne l'ensemble des applications de E dans F. $\mathcal{P}(E)$ désigne l'ensemble de toutes les parties de E, et $\mathcal{P}_k(E)$ l'ensemble de ses parties à k éléments.

Proposition : $\left|F^E\right| = |F|^{|E|}$

Définition : la *fonction caractéristique* χ_A d'une partie A d'un ensemble E est l'application $E \to \{0, 1\}$ définie par $\chi_A(x) = 1$ si $x \in A$, et $\chi_A(x) = 0$ sinon.

Proposition : $A \mapsto \chi_A$ est une bijection de $\mathcal{P}(E)$ sur $\{0, 1\}^E$, donc $|\mathcal{P}(E)| = 2^{|E|}$.

Lemme du berger : soit E et F deux ensembles tels qu'il existe une surjection $E \twoheadrightarrow F$ vérifiant : $\forall x, y \in F, |f^{-1}(x)| = |f^{-1}(y)|$. Alors, si k désigne le cardinal commun des images réciproques des éléments de F, $|E| = k \cdot |F|$.

Proposition : soit E et F deux ensembles de cardinal respectif m et n ; le nombre d'injections de E dans F est égal à $n(n-1)\dots(n-m+1)$. En particulier, si $m = n$, le nombre de bijections de E sur F est $n!$.

Notation : $n(n-1)\dots(n-m+1)$, appelée m^e *factorielle descendante* de n, est notée $(n)_m$.

Pour les surjections, c'est plus compliqué.

IV. « k parmi n »

Définition : On appelle
- *arrangement* de k éléments parmi n tout k-uplet d'éléments distincts de $[\![1, n]\!]$;
- *arrangement à répétitions* de k éléments parmi n tout k-uplet d'éléments de $[\![1, n]\!]$;
- *combinaison* de k éléments parmi n toute partie à k éléments de $[\![1, n]\!]$;
- *combinaison à répétitions* de k éléments parmi n toute *multipartie*[1] à k éléments de $[\![1, n]\!]$.

Notation : nombres d'arrangements : A_n^k, de combinaisons (appelés *coeeficients binomiaux*) : $\binom{n}{k}$ ou C_n^k, de combinaisons à répétitions : $\left(\!\binom{n}{k}\!\right)$.

Nombre de façons de sélectionner k éléments parmi n :

	arrangements	combinaisons
simples	$(n)_k$	$\binom{n}{k}$
à répétitions	n^k	$\left(\!\binom{n}{k}\!\right) = \binom{n-k+1}{k}$

Propriétés des coefficents binomiaux :

- annulation : $\binom{n}{k} = 0$ si $k < 0$ ou $k > n$
- élimination : $k\binom{n}{k} = n\binom{n-1}{k-1}$
- symétrie : $\binom{n}{k} = \binom{n}{n-k}$
- somme totale : $\sum_k \binom{n}{k} = 2^n$
- relation de Pascal : $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
- convolution de Vandermonde : $\sum_k \binom{p}{k}\binom{q}{n-k} = \binom{p+q}{n}$; en particulier, $\sum_k \binom{n}{k}^2 = \binom{2n}{n}$.

[1] une *multipartie* A d'un ensemble E peut être définie à partir de sa fonction caractéristique, qui est une application de E dans $\mathbb{N}$; les *éléments* de A sont les éléments de E dont l'image est non nulle, et la *multiplicité* d'un élément de A est son image par cette application ; enfin, le *cardinal* de A est la somme des multiplicités de ses éléments.

Formule du binôme :

$$\forall x, y, \quad (x+y)^n = \sum_k \binom{n}{k} x^k y^{n-k}$$

Généralisation : coefficients multinomiaux

Propriété : le nombre de mots de longueur n sur un alphabet à k lettres $\{a_1, \ldots, a_k\}$ avec n_i occurrences de la lettre a_i est égal à :

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\cdots\binom{n_{k-1}+n_k}{n_{k-1}} = \frac{n!}{n_1! n_2! \ldots n_k!}$$

Notation : $\binom{n}{n_1, n_2, \ldots, n_k}$

Formule du multinôme :

$$\forall x_1, \ldots, x_k, \quad (x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{(n_1,n_2,\ldots,n_k)\in\mathbb{N}^* \\ n_1+n_2+\cdots+n_k=n}} \binom{n}{n_1, n_2, \ldots, n_k} \cdot x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k}$$

V. Application à la génération exhaustive

Chapitre 2 : Permutations

I. Généralités

Définition : une *permutation* de taille $n \in \mathbb{N}$ est une bijection de $[\![1, n]\!]$ dans lui-même ; plus généralement, une bijection d'un ensemble E est une bijection de E dans lui-même. L'ensemble des permutations de taille n est appelé *groupe symétrique d'ordre* n (ou encore n^{e} groupe symétrique).

Notation : $\mathfrak{S}_n$; $\mathfrak{S}(E)$

Propriété : $|\mathfrak{S}_n| = n!$

Notation bilinéaire : une permutation $\sigma \in \mathfrak{S}_n$ peut être décrite par $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$, et plus généralement une permutation d'un ensemble E par une matrice à deux lignes dont chaque colonne représente un couple $(x, \sigma(x))$ différent.

Notation sous forme d'un mot : dans le cas d'une permutation de $[\![1, n]\!]$, on peut faire sans ambiguïté l'économie de la première ligne de la matrice, et représenter σ par le mot $\sigma = \sigma(1)\ \sigma(2)\ \dots\ \sigma(n)$ (mot sur l'alphabet $[\![1, n]\!]$ avec exactement une occurrence de chaque lettre de l'alphabet).

Les éléments de $\mathfrak{S}_n$ peuvent être *composés* entre eux, ce qui permet de munir l'ensemble des permuations de taille n d'un produit interne, pour lequel chaque permutation σ possède une *inverse* telle que $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id} (= 1\ 2\ 3\ \dots\ n)$ (ce qui donne une structure de groupe, d'où la terminologie de *groupe* symétrique).

Notation : si $\sigma, \tau \in \mathfrak{S}_n$, $\sigma\tau = \sigma \circ \tau$, *i.e.* $\sigma\tau(i) = \sigma(\tau(i))$.

Exemple : soit $\sigma = 3\ 1\ 4\ 2\ 5$; alors $\sigma^{-1} = 2\ 4\ 1\ 3\ 5$.

Définition : un *point fixe* d'une permutation σ est un élément i tel que $\sigma(i) = i$; le *support* de σ est l'ensemble des éléments qui ne sont pas des points fixes de σ.

Notation : $\mathrm{Supp}(\sigma)$

Propriété : soit σ et τ telles que $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\tau) = \emptyset$. Alors $\sigma\tau = \tau\sigma$.

ATTENTION ! ! ! ce n'est pas (du tout) le cas en général ; par exemple, si $\sigma = 2\ 3\ 4\ 1$ et $\tau = 2\ 1\ 3\ 4$, $\sigma\tau = 3\ 2\ 4\ 1$ tandis que $\tau\sigma = 1\ 3\ 4\ 2$.

Définition : *itérer* une permutation, c'est la composer plusieurs fois avec elle-même. On appelle *orbite de i sous σ* l'ensemble formé des images itérées de i par σ : $\{s^k(i) | k \in \mathbb{N}\}$. On appelle *orbite de σ* toute orbite d'un élément i sous σ.

Propriété : les orbites de σ forment une partition de $[\![1, n]\!]$

Définition : On appelle *ordre* de i le cardinal de son orbite ; c'est aussi le plus petit entier $k > 0$ tel que $\sigma^k(i) = i$.

Définition : on appelle *cycle de longueur ℓ* ou *ℓ-cycle* toute permutation ayant une seule orbite non triviale (*i.e.* de cardinal au moins 2).

Notation : soit $\gamma \in \mathfrak{S}_n$ un ℓ-cycle, et i un élément de son support ; alors l'orbite non triviale de γ est $\{i, \gamma(i), \ldots, \gamma^\ell(i)\}$. On note alors $\gamma = (i\ \gamma(i)\ \ldots\ \gamma^\ell(i))$. Cette notation n'est pas unique, puisqu'elle dépend du choix de l'élément i parmi les ℓ éléments du support de γ.

Exemple : $\sigma = 2\ 3\ 4\ 1 = (1\ 2\ 3\ 4) = (2\ 3\ 4\ 1) = (3\ 4\ 1\ 2) = (4\ 1\ 2\ 3)$

Proposition : toute permutation s'écrit de façon unique (à l'ordre près des facteurs, qui commutent) comme produit de cycles à supports disjoints. Les supports de ces cycles sont les orbites non triviales de la permutation produit.

Exemple : $\sigma = 4\ 3\ 5\ 1\ 2 = (1\ 4)\ (2\ 3\ 5) = (3\ 5\ 2)\ (4\ 1) = \ldots$

C'est ce qu'on appelle la *notation cyclique* des permutations.

Proposition : le nombre de permutations de taille n à k orbites, noté $c(n,k)$, vérifie : $c(0,0) = 1$ et $c(n,k) = (n-1)c(n-1,k) + c(n-1,k-1)$. On l'appelle *nombre de Stirling de 1re espèce non signé*.

Définition : une *transposition* est un 2-cycle ; un *grand cycle* ou une *permutation circulaire* est un cycle sans point fixe.

Propriété : dans $\mathfrak{S}_n$ le nombre de transpositions est $\binom{n}{2}$, le nombre de grands cycles est $(n-1)!$, et plus généralement le nombre de ℓ-cycles est $\binom{n}{\ell}(\ell-1)! = \frac{(n)_\ell}{\ell}$.

Proposition : toute permutation peut s'écrire comme produit de transpositions (à supports a priori non disjoints, et le produit n'est donc pas commutatif en général). On dit que les transpositions *engendrent* $\mathfrak{S}_n$.

II. Inversions ; génération ; tris

Définition : un couple (i,j) est une *inversion* de $\sigma \in \mathfrak{S}_n$ si $i < j$ et $\sigma^{-1}(i) < \sigma^{-1}(j)$, *i.e.* $\sigma = \ldots i \ldots j \ldots$. Définition concurrente, qui revient à considérer que l'inversion est concerne les positions et non les éléments dans le mot : si $i < j$ et $\sigma(i) > \sigma(j)$.

Notation : on note respectivement $\mathcal{I}(\sigma)$ et $I(\sigma)$ l'ensemble des inversions de σ et son cardinal.

Notation : on note $\tilde{\sigma}$ la permutation « miroir » de σ, *i.e.* la permutation telle que $\tilde{\sigma}(i) = \sigma(i)$.

Propriété : $I(\sigma) = I(\sigma^{-1})$; $I(\sigma) + I(\tilde{\sigma}) = \binom{n}{2}$, donc la valeur moyenne du nombre d'inversions est $\frac{1}{4}n(n-1)$.

Définition : le *code de Lehmer* d'une permutation $\sigma \in \mathfrak{S}_n$ est le n-uplet $c(\sigma) = (c_1(\sigma), \ldots, c_n(\sigma))$ tel que $\forall i \in [\![1,n]\!]$, $c_i(\sigma) = \#\{j > i | \sigma(j) < \sigma(i)\}$ (*i.e.* le nombre d'éléments au-delà de la i^{e} place plus petits que l'élément qui s'y trouve). La *table d'inversion* de σ est le n-uplet $t(\sigma) = (t_1(\sigma), \ldots, t_n(\sigma))$ tel que $\forall i \in [\![1,n]\!]$, $t_i(\sigma) = \#\{j < \sigma^{-1}(i) | \sigma(j) > i\}$ (*i.e.* le nombre d'éléments à gache de i plus grands que i).

Propriété : $t(\sigma) = c(\sigma^{-1})$ (et donc $c(\sigma) = t(\sigma^{-1})$).

Propriété : l'application $\sigma \mapsto c(\sigma)$ (ainsi que l'application $\sigma \mapsto t(\sigma)$) réalise une bijection de $\mathfrak{S}_n$ sur $[\![0, n-1]\!] \times [\![0, n-2]\!] \times \cdots \times [\![0, 1]\!] \times [\![0, 0]\!]$.

Application 1 : algorithme de génération (exhaustive ou aléatoire)

Application 2 : complexités des algorithmes de tri : par exemple, le tri à bulles réalise exactement $I(\sigma)$ échanges pour trier la permutation σ, tandis que le tri par insertion fait exactement $I(\sigma) + n - 1$ comparaisons.

III. Dérangements. Principe d'inclusion-exclusion

Définition : un *dérangement* est une permutation sans point fixe.

Notation : D_n le nombre de dérangements de taille n.

Proposition : $n! = \sum_{k=1}^{n} \binom{n}{k} D_k$

Proposition : $D_n = (n-1)[D_{n-1} + D_{n-2}]$; donc $D_n = nD_{n-1} + (-1)^n$; donc $D_n = n! \sum_{k=1}^{n} \frac{(-1)^k}{k!}$.

Principe d'inclusion-exclusion : Soit $A_1, \ldots, A_n$ des parties d'un ensemble E ; alors le complémentaire de $A_1 \cup \cdots \cup A_n$ a pour cardinal :

$$\sum_{I \in [\![1,n]\!]} (-1)^{|I|} |A_I|,$$

où $A_I = \bigcap_{i \in I} A_i$, $A_\emptyset = E$.

En particulier, si $n = 2$, $|E| - |A \cup B| = |E| - |A| - |B| + |A \cap B|$, soit encore : $|A \cup B| + |A \cap B| = |A| + |B|$.

Application 1 : cela permet de retrouver le nombre de dérangements, en prenant $E = \mathfrak{S}_n$, $A_i = \{\sigma \in \mathfrak{S}_n | \sigma(i) = i\}$: alors $D_n = |\overline{A_1 \cup \cdots \cup A_n}$, avec $|A_i| = (n-1)!$ et plus généralement $|A_I| = (n - |I|)!$, ce qui donne :

$$D_n = \sum I \in [\![1, n]\!] (-1)^{|I|} (n - |I|)! = \sum_{i=0}^{n} \binom{n}{i} (-1)^i (n-i)! = \sum_{i=0}^{n} (-1)^i \frac{n!}{i!}.$$

Application 2 : dénombrement des surjections de $[\![1, n]\!]$ sur $[\![1, k]\!]$
Soit $E = [\![1, k]\!]^{[\![1,n]\!]}$ et $A_i = \{f \in E | f^{-1}(i) = \emptyset\}$; alors $|A_i| = (k-1)^{|n|}$, et plus généralement $|A_I| = (k - |I|)^n$, donc le nombre $\mathcal{S}(n, k)$ de surjections de $[\![1, n]\!]$ dans $[\![1, k]\!]$ est égal à :

$$\mathcal{S}(n, k) = \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n.$$

En particulier, $\mathcal{S}(n, n) = n! \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n-i)^n$.

Définition : On appelle *nombre de Stirling de 2e espèce* le nombre de partitions de $[\![1, n]\!]$ en k parts non vides.

Notation : $S(n,k)$

Propriété : $k!S(n,k) = \mathcal{S}(n,k)$.

Propriété : $S(n,k) = kS(n-1,k) + S(n-1,k-1)$.