Leçon 145 - Méthodes combinatoires, problèmes de dénombrement.

I. Problèmes introductifs

1) Tirages [de Biasi]

On tire de différentes manières p boules dans une urne de n boules et on dénombre le nombre de tirages possibles.

- tirages ordonnés (successifs) avec remise : $\boxed{n^p}$

revient à dénombrer les applications de $[\![1,p]\!]$ dans $[\![1,n]\!]$

- tirages ordonnés sans remise : $\boxed{n(n-1)\cdots(n-p+1) := A_n^p}$

↳ revient à dénombrer les injections de $[\![1,p]\!]$ dans $[\![1,n]\!]$

- tirages non ordonnés sans remise : $\boxed{\frac{A_n^p}{p!} = C_n^p}$

↳ on ne tient pas compte de l'ordre, toutes les p-parties en bijection représentent le même tirage, or ces bijections sont au nombre de $p!$.

Relations vérifiées par les C_n^p :

- $C_n^p = C_n^{n-p}$
- $C_n^p = C_{n-1}^p + C_{n-1}^{p-1}$ "triangle de Pascal"

Applications des "arrangements" et "combinaisons" :

- dim de {polynômes homogènes de degré d à n variables} : C_{n+d-1}^{n-1}
- cardinal d'une classe de conjugaison de S_n :

exemple : nombre de 3-cycles de S_4 : $\frac{A_4^3}{3} = 8$

2) Combien peut-on écrire de nombres de trois chiffres contenant au moins l'un des chiffres 0, 3, 6, 9 ?

$E = \{$nombres à 3 chiffres$\}$, $A = \{$nombres à 3 chiffres contenant au moins 0, 3, 6 ou 9$\}$

alors $|A| = |E| - |\complement_E A|$

$\complement_E A = \{$nombres à 3 chiffres écrits avec les seuls chiffres 1, 2, 4, 5, 7, 8$\}$

$$\left.\begin{array}{l} |\complement_E A| = 6^3 \\ |E| = 900 \end{array}\right\} \quad |A| = 684$$

- On a utilisé : Soit A et B 2 parties finies d'un ensemble, alors $\boxed{|A\cup B| = |A| + |B| - |A\cap B|}$.
- Qui se généralise en la formule du crible :

Soit $k \in \mathbb{N}^*$ et $(E_i)_{i\in[\![1,k]\!]}$ une famille finie d'ensembles finis. Alors

$$\left|\bigcup_{i=1}^{k} E_i\right| = \sum_{i=1}^{k}\left[(-1)^{i+1}\sum_{1\le j_1<\dots<j_i\le k}\left|\bigcap_{q=1}^{i} E_{j_q}\right|\right]$$

- application : nombre de surjection de $[\![1,p]\!]$ dans $[\![1,n]\!]$:

$$\begin{cases} 0 & \text{si } p<n \\ n! & \text{si } p=n \\ \sum_{k=0}^{n}(-1)^{n-k}C_n^k k^p & \text{si } p>n \end{cases}$$

3) Calcul de certains cardinaux [Perrin]

Quel est le cardinal de $GL_n(\mathbb{F}_q)$?

idée : $GL_n(\mathbb{F}_q) \xleftrightarrow{\text{bijection}} \{$matrices inversibles de $\mathcal{M}_n(\mathbb{F}_q)\}$

Lemme des Bergers : Soit A et B deux ensembles finis, et φ une application de A ds B, si $\forall x\in B$ $|\varphi^{-1}(x)| = n$, alors : $|A| = n\,|B|$

↳ Si A et B sont en bijection $|A| = |B|$

Ainsi, découlent :
- $|GL_n(\mathbb{F}_q)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$
- $|SL_n(\mathbb{F}_q)| = |GL_n(\mathbb{F}_q)|/_{q-1}$
- $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|$
- $|PSL_n(\mathbb{F}_q)| = |PGL_n(\mathbb{F}_q)| / \text{pgcd}(n, q-1)$

Application : isomorphismes remarquables :
- $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PGL_2(\mathbb{F}_2) \simeq S_3$
- $PGL_2(\mathbb{F}_3) \simeq S_4$, $PSL_2(\mathbb{F}_3) \simeq \mathcal{A}_4$
- $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq \mathcal{A}_5$
- $PGL_2(\mathbb{F}_5) \simeq S_5$, $PSL_2(\mathbb{F}_5) \simeq \mathcal{A}_5$

- En considérant l'application : $\mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$ $x \longmapsto x^2$
on détermine le nombre de carré de $\mathbb{F}_q^*$: $\frac{q-1}{2}$.

4) Problème du scrutin [FF]

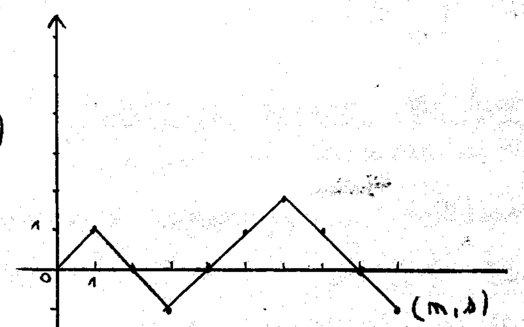
Dans un scrutin il y a p bulletins pour le candidat P et q pour Q. On suppose $p > q$. Quelle est la probabilité pour que durant ~~tt~~ le dépouillement, P soit toujours en tête ?

- On modélise le dépouillement par une suite finie d'élts de $\{+1,-1\}$: w . $w_i = 1$ si le i-ème bulletin est pour P, -1 sinon.

on pose : $n = p+q$, $\quad s_k = w_1 + \dots + w_k$, $\quad s = p-q$

on va représenter w comme un chemin de $(0,0)$ à (n,s) en joignant les pts $(0,0), (1,s_1), \dots, (i,s_i)$.

→ idée : dénombrer le nombre de chemins joignant $(0,0)$ à (n,s) et le nombre qui restent strictement au-dessus de l'axe horizontal, car le rapport du second sur le premier donne la proba cherchée.



exemple : $w = \{1,-1,-1,1,1,1,1,-1,-1,-1\}$

- nbre de chemins joignant $(0,0)$ à (n,s) : $\binom{p+q}{p}$ où $p = \frac{n+s}{2}$
- nbre qui reste strictement au-dessus de l'axe horizontal ?

<u>principe de réflexion :</u>
Le nombre de chemins allant de 2 pts A et B (du m côté de l'axe) qui touchent ou traversent l'axe horizontal est égal au nombre allant du symétrique de A /. à l'axe à B.

↳ il y a $\frac{p-q}{p+q}\binom{p+q}{p}$ chemins restant strict au-dessus.

II. Nombre de façons de colorier un cube ?

Soit G un groupe fini, E un ensemble fini, $O_1 \dots O_k$ les orbites de E sous l'action de G. $\forall i \in [\![1,k]\!]$ on prend $x_i \in O_i$
$G_{x_i} = \{g \in G \,/\, g \cdot x_i = x_i\}$.

a) Equations des classes :

- $|E| = \sum_{i=1}^{k} |O_i|$ (crible)
- $|O_i| = |G| / |G_{x_i}|$ (Lemme des Bergers)

b) Formule de Burnside

- Le nombre d'orbites est $k = \frac{1}{|G|} \sum_{g \in G} |\mathrm{fix}(g)|$
où $\mathrm{fix}(g) = \{x \in E \,/\, g \cdot x = x\}$

<u>Application au coloriage du cube :</u> [Lehman]

Soit $\mathcal{G}$ le groupe des isométries du cube, Φ l'ensemble des colorations : applications de $[\![1,6]\!]$ (faces) dans $\{c_1, \dots, c_m\}$ (couleurs).
Si $\varphi_1, \varphi_2 \in \Phi$ sont telles qu'il existe $g \in \mathcal{G}$: $\varphi_1 = \varphi_2 \circ g$ alors φ_1 et φ_2 représente le même coloriage.
On considère donc l'action de $\mathcal{G}$ sur Φ, et le nombre de coloriages k est le nombre d'orbites de cette action. On trouve
$$k = \frac{1}{24}\left(m^6 + 3m^4 + 12m^3 + 8 \cdot m^2\right).$$

<u>Application aux ss-groupes finis du groupe des isométries</u> [Combes]

proposition : Soit G un sous-groupe fini, d'ordre $n \geq 2$, du groupe des déplacements de l'espace affine euclidien $\mathcal{E}_3$. Alors G est isomorphe à $\mathbb{U}_n$, $D_{n/2}$, ou à l'un des 3 groupes des déplacements qui conservent l'un des 5 polyèdres réguliers i.e. $\mathcal{A}_4$, S_4, ou $\mathcal{A}_5$.

III. Problèmes mettant en jeu des séries formelles

Soit K un corps commutatif, et $K[[X]]$ l'algèbre des séries formelles dont on rappelle la multiplication :
$S = (a_n)_{n \in \mathbb{N}} \in K[[X]]$ $\quad T = (b_n)_{n \in \mathbb{N}} \in K[[X]]$ alors $(ST)_n = c_n = \sum_{p+q=n} a_p b_q$

1) Nombre de façons de faire la monnaie d'une certaine somme avec des valeurs de pièces données [OXE 2]

Soit $\alpha_1, \dots, \alpha_p$ des entiers non nuls premiers entre eux, S_n le nombre de solutions $(n_1, \dots, n_p) \in \mathbb{N}^p$ de l'équation :
$\alpha_1 n_1 + \dots + \alpha_p n_p = n$, $\quad n \in \mathbb{N}$.

On a $S_n \underset{\infty}{\sim} \dfrac{n^{p-1}}{\alpha_1 \cdots \alpha_p \, (p-1)!}$

- Dans certains cas, on peut calculer une valeur exacte : monnaie de 100 euros avec des pièces de 1, 2 et un billet de 5.

2) Nombre de manières d'écrire un entier comme somme d'entiers non nuls [OXE 2]

On note $p(n)$ ce nombre, et on remarque que les fonctions $(f_n)_n$ définit par : $f_n(t) = \prod_{k=1}^{n} \dfrac{1}{1-t^k}$, y donne accès :

$$f_n(t) = \prod_{k=1}^{n} \frac{1}{1-t^k} = \sum_{l=0}^{+\infty} \Big(\underbrace{\sum_{y_1+2y_2+\dots+ny_n = l} 1}_{= p(l) \text{ dès que } n \geq l \geq 1} \Big) t^l$$

Applications des $p(n)$:

- Le nombre de classes de similitudes d'endomorphismes nilpotents de $\mathcal{M}_n(\mathbb{R})$ est $p(n)$
- Le nombre de classes de conjugaison de S_n est $p(n)$

3) Nombre de partitions de $[\![1,n]\!]$

Soit $n \in \mathbb{N}$, et D_n le nombre de partitions de $[\![1,n]\!]$.

Alors $D_n = \dfrac{1}{e} \displaystyle\sum_{k \geq 0} \dfrac{k^n}{k!}$. (DEV)

4) Nombre de façons de parenthéser une suite de n termes [Taurel]

Soit E un ensemble muni d'une loi de composition interne notée multiplicativement et $x \in E$. On note p_n le nombre de parenthésages d'une suite de n termes égaux à x.

Les multiplications successives opèrent sur deux facteurs adjacents.

Exemple : $p_0 = 0$, $p_1 = 1$, $p_2 = 1$, $p_3 = 2$: $(xx)x$, $x(xx)$

$p_4 = 5$ $(xx)(xx)$, $((xx)x)x$, $(x(xx))x$, $x((xx)x)$, $x(x(xx))$

Les p_n sont appelés nbre de Catalan. On considère leur série génératrice : $S = \sum_{n \geq 0} p_n X^n$.

On remarque que $p_n = p_1 p_{n-1} + p_2 p_{n-2} + \dots + p_{n-1} p_1$

d'où notant $S^2 = \sum q_n X^n$ on a $q_0 = q_1 = 0$ et $q_n = p_n$ pour $n \geq 2$

d'où $S^2 - S + X = 0$.

L'intégrité de $\mathbb{C}[[X]]$ et la donnée de $p_1 = 1$ nous permet de déterminer S : $S = \frac{1}{2}\left[1 - (1-4X)^{1/2}\right]$ et donc de conclure que $p_n = \dfrac{1}{n} C_{2n-2}^{n-1}$ pour $n \geq 2$.

IV. Fonction de Möbius et nombre de polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$ [FG]

a) Définition et propriétés de la fonction de Möbius μ

déf : On définit $\mu : \mathbb{N}^* \longrightarrow \{0, 1, -1\}$ comme suit :

$\mu(1) = 1$ et $\mu(n) = \begin{cases} 0 & \text{si } n \text{ contient un facteur carré} \\ (-1)^r & \text{si } n = p_1 \cdots p_r \text{ où les } p_i \text{ sont premiers distincts} \end{cases}$

prop :
- Soit $n_1, n_2 \in \mathbb{N}^*$ avec $(n_1, n_2) = 1$ alors $\mu(n_1 n_2) = \mu(n_1)\mu(n_2)$
- $\forall n \in \mathbb{N}^*, n \neq 1$ $\displaystyle\sum_{d|n} \mu(d) = 0$
- "formule d'inversion de Möbius"

Soit $f : \mathbb{N}^* \to A$ où A désigne un groupe abélien noté additivement. On pose $g(n) = \sum_{d|n} f(d)$, alors :

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu(d)\, g\left(\frac{n}{d}\right)$$

b) Application aux polynômes irréductibles de $\mathbb{F}_q[X]$

Soit $n \in \mathbb{N}^*$, on note $I(n,q)$ le cardinal de l'ensemble des polynômes unitaires irréductibles de degré n sur $\mathbb{F}_q$, alors :

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$$ (DEV)

- [Taurel] : Patrice Tauvel - Cours d'algèbre
- [de Biasi] : Jean de Biasi - Math pour le Capes et l'agreg int.
- [OXE 2] : Oraux - X - ENS analyse 2
- [AG] : Arnold - Guessarian - Math pour l'info
- [Perrin] : Daniel Perrin - Cours d'Algèbre
- [FF] : Foata - Fuchs - Calcul des proba
- [FG] : Francinou - Gianella - Exos de math pour l'agreg - algèbre 1
- [Combes] : François Combes - algèbre et géométrie
- [Lehman] : Math pour l'étudiant de 1ère année - alg et géom (Lehman)

Autres développements possibles :

- coloriage du cube
- sous groupes finis du groupe des isométrie en dimension 3.
- Le III . 1.
- probabilité que deux nombres soit premier entre eux.
- traiter un pb de dénombrement avec [illegible] par ex nb de Catalan