P. Maurer
ENS Rennes

Leçon 190. Méthodes combinatoires, problèmes de dénombrement

Devs :

- Formule du crible par les involutions alternantes
- Récurrence et transience de la marche aléatoire sur $\mathbb{Z}$, $\mathbb{Z}^2$ et $\mathbb{Z}^3$

Références :

1. Biaisi, Mathématiques pour le CAPES et l'Agrégation Interne
2. Ulmer, Théorie des groupes
3. Perrin, Cours d'algèbre
4. Ouvrard, Probabilités
5. Garet, Probabilités et processus stochastiques
6. Norris, Markov chains
7. Un DM posé à LLG (bibliographie hélas introuvable)

On se donne E un ensemble.

1 Analyse combinatoire et méthodes de dénombrement

1.1 Ensembles finis

Définition 1. *On appelle cardinal de E, et on note $|E|$ la classe des ensembles en bijection avec E. On dit que E est fini s'il est en bijection avec $[\![1,n]\!]$ pour $n\in\mathbb{N}$, et dans ce cas, on note n son cardinal.*

Remarque 2. $\varnothing$ est fini, de cardinal 0 avec la convention $[\![1,0]\!]=\varnothing$.

Proposition 3. *Soit E et F deux sous-ensembles finis d'un ensemble S. Alors $E\cap F$ et $E\cup F$ sont finis et on a $|E\cap F|=|E|+|F|-|E\cup F|$.*

Proposition 4. *Si $(E_i)_{i\in[\![1,n]\!]}$ est une famille de sous-ensembles finis disjoints d'un ensemble S, alors on a $|\bigcup_{i=1}^n E_i|=\sum_{i=1}^n |E_i|$.*

Proposition 5. *Si $(E_i)_{i\in[\![1,n]\!]}$ est une famille de sous-ensembles finis d'un ensemble S, alors on a $|\bigcup_{i=1}^n E_i|\leq\sum_{i=1}^n |E_i|$.*

Remarque 6. L'application $|\cdot|$ qui à un ensemble de $\mathcal{P}(\mathbb{N})$ associe son cardinal est une mesure sur l'espace $(\mathbb{N},\mathcal{P}(\mathbb{N}))$.

Théorème 7. *Si $A_1,\ldots,A_p$ sont des ensembles finis, leur produit cartésient $\prod_{i=1}^p A_i$ est fini, et vérifie $|\prod_{i=1}^p A_i|=\prod_{i=1}^p |A_i|$.*

Proposition 8. *Si E et F sont deux ensembles finis, l'ensemble des fonctions de E vers F est un ensemble fini de cardinal $|F|^{|E|}$.*

Corollaire 9. *On a $|\mathcal{P}(E)|=2^{|E|}$.*

Exemple 10. Il y a $2^6=64$ signes possibles dans l'alphabet braille.

1.2 Arrangements, permutations, et combinaisons

On considère un ensemble fini E de cardinal $n\in\mathbb{N}^*$.

Définition 11. *Soit $p\leq n$. On appelle arrangement de E une injection $[\![1,p]\!]\to E$.*

Proposition 12. *Le nombre d'arrangements de E est $A_n^p=\dfrac{n!}{(n-p)!}$.*

Définition 13. *On appelle permutation de E une bijection $[\![1,n]\!]\to E$ (remarquons que c'est un cas particulier d'arrangement). On note $\mathcal{S}(E)$ l'ensemble des permutations de E.*

Proposition 14. *Le nombre de permutations de E est $|\mathcal{S}(E)|=A_n^n=n!$.*

Définition 15. *On appelle combinaison de E à p éléments tout sous ensemble de E à p éléments. On note $\binom{n}{p}$ le nombre de combinaisons de E à p éléments.*

Proposition 16. *On a $\binom{n}{p}=\dfrac{n!}{p!(n-p)!}$.*

Proposition 17. *Pour $n\geq 1$ et $1\leq p\leq n$, on a :*

- $\binom{n}{p}=\binom{p}{n-p}$,
- $\binom{n}{p}=\binom{n-1}{p}+\binom{n-1}{p-1}$ *(formule du triangle de Pascal),*
- $\binom{n}{p}=\frac{n}{p}\binom{n-1}{p-1}=\frac{n}{n-p}\binom{n-1}{p}=\frac{n-p+1}{p}\binom{n}{p-1}$.

Exemple 18. Il y a $\binom{n}{p}$ applications strictement croissantes de $[\![1,p]\!]$ vers $[\![1,n]\!]$.

Lemme 19. *Si $f\colon[\![1,p]\!]\to[\![1,n]\!]$ est une application croissante, alors $g\colon x\mapsto f(x)+x-1$ est une application strictement croissante de $[\![1,p]\!]$ vers $[\![1,n-p+1]\!]$.*

Corollaire 20. *Il y a* $\binom{n-p+1}{p}$ *applications croissantes de* $[\![1,p]\!]$ *vers* $[\![1,n]\!]$.

Proposition 21. *(Binôme de Newton).*
Soit A *un anneau,* $a,b\in A$ *qui commutent et* $n\in\mathbb{N}$. *On a*

$$(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k}.$$

Exemple 22. La formule $(X+1)^n=\sum_{k=0}^{n}\binom{n}{k}X^k$ permet de retrouver les formules :

- $\sum_{k=1}^{n}k=\frac{n(n+1)}{2}$,
- $\sum_{k=1}^{n}k^2=\frac{n(n+1)(2n+1)}{6}$,
- $\sum_{k=1}^{n}k^3=\left(\frac{n(n+1)}{2}\right)^2$.

Exemple 23. Le nombre σ_p^n de surjections de $[\![1,\,n]\!]$ dans $[\![1,\,p]\!]$ est $\sigma_p^n=\sum_{k=0}^{p}(-1)^{p-k}\binom{p}{k}k^n$.

1.3 Dénombrement par involutions alternantes

Notation 24. *Pour* $f\colon E\to E$ *une application et* $A\subset E$, *on notera* $F_f(A)$ *l'ensemble des points fixes de* f *sur* A : $F_f(A)=\{x\in A:\ f(x)=x\}$.

Définition 25. *Soit* E *un ensemble fini, partitionné en* $A_+\sqcup A_-$.
On appelle involution alternante sur E *une application* $f\colon E\to E$ *vérifiant :*

- $f\circ f=\mathrm{Id}_E$,
- $\forall x\in A_+\setminus F_f(A_+)\quad f(x)\in A_-$,
- $\forall x\in A_-\setminus F_f(A_-)\quad f(x)\in A_+$.

Développement 1 :

Théorème 26. *(Principe du dénombrement par involutions alternantes).*
On a $|F_f(A_+)|+|F_f(A_-)|=|A_+|+|A_-|$.

Application 27. *(Formule du crible via les involutions alternantes).*
Soit E *un ensemble fini et* $A_1,\ldots,A_n\subset E$. *Alors*

$$\left|\bigcup_{i=1}^{n}A_i\right|=\sum_{\substack{I\subset\mathcal{P}([\![1,n]\!])\\ I\neq\varnothing}}(-1)^{|I|-1}\left|\bigcap_{i\in I}A_i\right|.$$

Application 28. *(Chemins de Catalan).*
Soit $n\in\mathbb{N}^*$. *On étudie les chemins du plan à* $n+1$ *sommets* $M_0,\ldots,M_n$, *qu'on note* $(M_0,\ldots,M_n)$, *tels que pour tout* $k\in[\![1,n]\!]$, $\overrightarrow{M_{k-1}M_k}=(1,0)$ *ou* $\overrightarrow{M_{k-1}M_k}=(0,1)$.
Alors le nombre C_n *de tels chemins joignant* $(0,0)$ *à* (n,n) *tels que tous les sommets aient une abscisse supérieure ou égale à leur ordonnée vaut* $C_n=\frac{1}{n+1}\binom{2n}{n}$.
Le nombre C_n *est appelé nombre de Catalan.*

Théorème 29. *(Bijection de Garsia-Milne).*
Soit A *et* B *des ensembles finis, partitionnés en* $A=A_+\sqcup A_-$ *et* $B_+\sqcup B_-$, f *une involution alternante de* A *et* g *une involution alternante de* B. *On suppose que* $F_f(A_-)=F_g(B_-)=\varnothing$, *et qu'il existe une bijection* $\varphi\colon A\to B$ *telle que* $\varphi(A_+)\subset B_+$ *et* $\varphi(A_-)\subset B_-$.
Alors il existe une bijection entre $F_f(A_+)$ *et* $F_g(B_+)$.

2 Dénombrement en algèbre

2.1 Dénombrement sur les corps finis

Définition 30. *On note, pour* p *premier et* $n\in\mathbb{N}$, $U_n(\mathbb{F}_p)$ *le sous-groupe de* $\mathrm{GL}_n(\mathbb{F}_p)$ *constitué des matrices triangulaires supérieures inversibles.*

Proposition 31. *Soit* p *un nombre premier et* $n\in\mathbb{N}$. *Alors on a :*

- $|\mathrm{GL}_n(\mathbb{F}_p)|=(p^n-1)\cdots(p^n-p^{n-1})=m\,p^{\frac{n(n-1)}{2}}$,
- $|\mathrm{SL}_n(\mathbb{F}_p)|=(p^n-1)\cdots(p^n-p^{n-2})\cdot p^{n-1}$,
- $|U_n(\mathbb{F}_p)|=p^{\frac{n(n-1)}{2}}$.

Où $m=(p-1)\cdots(p^n-1)$ *est premier avec* p.

Soit p un nombre premier et $q=p^n$ avec $n\in\mathbb{N}^*$.

Proposition 32. *On suppose* $p>2$ *et on se donne* $a\in\mathbb{F}_q^*$. *Alors*

$$a^{\frac{q-1}{2}}=\begin{cases}1 & \text{si } a \text{ est un carré dans } \mathbb{F}_q^*\\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q^*\end{cases}.$$

Définition 33. *On définit le symbole de Legendre pour* $p>2$ *et* $a\in\mathbb{F}_p$ *par*

$$\left(\frac{a}{p}\right)=\begin{cases}1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^*,\\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^*,\\ 0 & \text{si } a=0.\end{cases}$$

Proposition 34. *Pour $a \neq 0$ on a $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$. En particulier, le symbole de Legendre est multiplicatif, au sens où $\left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.*

Proposition 35. *Soit p un nombre premier impair et a un élément de $\mathbb{F}_p^*$. On a*

$$|\{x \in \mathbb{F}_p \,:\, ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right).$$

Théorème 36. *(Loi de réciprocité quadratique)*
Soit p et q deux nombres premiers impairs distincts. Alors on a

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Exemple 37. Calcul du symbol de Legendre :
$\left(\frac{23}{59}\right) = (-1)^{11.29} \left(\frac{59}{23}\right) = -\left(\frac{13}{23}\right) = \cdots = \left(\frac{2}{3}\right) = -1.$

2.2 Dénombrement en théorie des groupes

Définition 38. *Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. On dit que $H < G$ est un p-Sylow de G si c'est un sous-groupe d'ordre p^α.*

Proposition 39. *Le groupe $\mathrm{GL}_n(\mathbb{F}_p)$ admet pour p-Sylow le sous-groupe $U_n(\mathbb{F}_p)$.*

Théorème 40. ***(Sylow)***
Soit G un groupe d'ordre $p^\alpha m$ avec $p \nmid m$. Alors :

1. *G possède au moins un p-Sylow.*
2. *Les p-Sylow sont tous conjugués entre eux.*
3. *En notant k le nombre de p-Sylow, on a $k \equiv 1 \pmod{p}$ et k divise m.*

Proposition 41. *(Formule des classes)*
Soit G un groupe fini qui agit sur un ensemble X fini. On note $O(x)$ l'orbite d'un élément $x \in X$ et G_x le stabilisateur de x dans G. Alors :

1. *Pour tout $x \in X$, on a $|O(x)| = [G : G_x]$.*
2. *Soit $O(x_1), \ldots, O(x_q)$ les orbites distinctes. On a*

$$|X| = \sum_{i=1}^{q} |O(x_i)| = \sum_{i=1}^{q} \frac{|G|}{|G_{x_i}|}.$$

Définition 42. *On appelle ensemble des points fixes de X sous G l'ensemble :*

$$X^G = \{x \in X \,:\, \forall g \in G \quad g.x = x\}$$

Proposition 43. *On suppose que G est un p-groupe et que X est fini. Alors on a :*

$$|X| \equiv |X^G| \pmod{p}$$

Corollaire 44. *Soit p un nombre premier. Alors tout groupe fini G de cardinal p^2 est abélien, et plus précisément isomorphe à $(\mathbb{Z}/p\mathbb{Z})^2$ ou bien à $\mathbb{Z}/p^2\mathbb{Z}$.*

Proposition 45. *(Formule de Burnside).*
Soit G un groupe fini de cardinal n agissant sur X un ensemble fini de cardinal p. Alors

$$|O| = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}_X(g)|,$$

où O désigne l'ensemble des orbites sous l'action de G.

Exemple 46. Avec 4 perles bleues, 3 blances et 2 vertes, on peut faire 76 colliers.

3 Dénombrement en probabilités

3.1 Probabilités sur un ensemble fini

On se donne Ω un ensemble fini.

Définition 47. *La mesure $\mathbb{P}$ définie sur Ω par $\mathbb{P}(A) = \frac{|A|}{|\Omega|}$ est une probabilité sur $(\Omega, \mathcal{P}(\Omega))$, appelée probabilité uniforme. Elle attribue la même valeur à tout évènement élémentaire $\{\omega\} \subset \Omega$.*

Exemple 48. On lance n fois un dé équilibré. La probabilité de l'évènement A_k : « On obtient k fois le chiffre 6 », où $k \in [\![0, 6]\!]$, vaut $\mathbb{P}(A_k) = \binom{n}{k} \frac{5^{n-k}}{6^n}$.

Définition 49. *On dit qu'une variable aléatoire X à valeurs dans $(\mathbb{N}, \mathcal{P}(\mathbb{N}))$ suit une loi de Bernouilli $\mathcal{B}(p)$ de paramètre p si $\mathbb{P}(X = 0) = p$ et $\mathbb{P}(X = 1) = 1 - p$.*

Proposition 50. *Si $X_1, \ldots, X_n \sim \mathcal{B}(p)$ sont indépendantes, alors la loi de $X = X_1 + \cdots + X_n$ est donnée par $\mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$ pour $k \in [\![0, n]\!]$. On dit que X suit une loi binomiale de paramètre (n, p).*

3.2 Récurrence de la marche aléatoire simple

On commence par rappeler la formule du multinôme de Newton.

Définition 51. *On note* $\binom{n}{i_1,\ldots,i_k}$ *le nombre de partitions ordonnées d'un ensemble de* n *éléments en* k *ensembles de cardinal respectif* $i_1,\ldots,i_k$.

Proposition 52. *On a* $\binom{n}{i_1,\ldots,i_k}=\frac{n!}{i_1!\cdots i_k!}$.

Théorème 53. *(Formule du multinôme).*
Soit $n,k\in\mathbb{N}$ *et* $x_1,\ldots,x_k$ *des éléments d'un anneau* A *commutatif. Alors*

$$(x_1+\cdots+x_k)^n=\sum_{i_1+\cdots+i_k=n}\binom{n}{i_1,\ldots,i_k}x_1^{i_1}\cdots x_k^{i_k}.$$

Dans ce qui suit, on se donne un espace d'état E, un noyau de transition P et une chaîne de Markov $(\Omega,\mathcal{F},(\mathcal{F}_n)_{n\in\mathbb{N}},(\mathbb{P}_x)_{x\in E},X=(X_n)_{n\geq 0})$. On se donne aussi un élément $x\in E$.

Définition 54. *On définit le nombre* N_x *de visites en* x *et le premier temps* T_x *de retour en* x *par*

$$N_x:=\sum_{n\in\mathbb{N}}\mathbf{1}_{\{X_n=x\}}\quad \text{et}\quad T_x:=\inf\{N\geq 1\ :\ X_N=x\}.$$

Proposition 55. *Une et une seule des deux situations suivantes a lieu :*

- $\mathbb{P}_x(T_x<\infty)=1$. *Dans ce cas,* $N_x=+\infty$ $\mathbb{P}_x$*-p.s. On dit que l'état* x *est récurrent.*
- $\mathbb{P}_x(T_x<\infty)<1$. *Dans ce cas,* $N_x<\infty$ $\mathbb{P}_x$*-p.s, et de plus,* $\mathbb{E}_x[N_x]=\frac{1}{\mathbb{P}_x(T_x=+\infty)}$. *On dit que l'état* x *est transient.*

Exemple 56.
Dans la marche aléatoire simple sur $\mathbb{Z}$, l'état zéro est récurrent.

Définition 57. *Soit* $x,y\in E$. *On dit que* x *mène à* y *et on note* $x\to y$ *si* $\mathbb{E}_x[N_x]>0$.
La relation $\to$ *est réflexive et transitive.*

Proposition 58. *Soit* $x,y\in E$. *On suppose que* $x\to y$ *et que* x *est récurrent. Alors* y *est récurrent, et* $y\to x$.

Définition 59. *On dit que la chaîne de Markov, ou le noyau de transition* P *est irréductible si*

$$\forall x,y\in E\quad x\to y.$$

Théorème 60. *(Classification des états d'une chaîne irréductible)*
Supposons la chaîne irréductible. Alors une et une seule des deux situations suivantes a lieu :

- *Tous les états sont récurrents, et* $\forall x\in E\quad \mathbb{P}_x(\forall y\in E, N_y=+\infty)=1$.
- *Tous les états sont transients, et* $\forall x\in E\quad \mathbb{P}_x(\forall y\in E, N_y<\infty)=1$.

Si E *est fini, alors on est toujours dans la première situation.*

Développement 2 :

Théorème 61. *(Récurrence de la marche aléatoire simple sur* $\mathbb{Z}^d$*)*
La marche aléatoire simple sur $\mathbb{Z}$ *et sur* $\mathbb{Z}^2$ *est récurrente. La marche aléatoire simple sur* $\mathbb{Z}^3$ *est transiente.*