145: méthode combinatoires. Problèmes de dénombrement

Pierre Lissy

April 25, 2010

1 Principes et outils fondamentaux

1.1 Cardinaux classiques

Proposition 1. *Si E est de cardinal n, $|P(E)| = 2^n$.*

Proposition 2. *Card $(F(E,F)) = |E|^{|F|}$.*

Proposition 3.
1. $|GL_n(F_q)| = (q^n - 1)\dots(q^n - q^{n-1})$
2. $|SL_n(F_q)| = (q^n - 1)\dots(q^n - q^{n-2})q^{n-1} =: N$
3. $|GL_n(F_q)| = N$
4. $|GL_n(F_q)| = N/pgcd(N, q-1)$

Proposition 4. $Card(\mathbb{Z}/nZ)^* = Card(k \leqslant n | pgcd(k,n) = 1) = \varphi(n)$

Proposition 5. *Formule du crible:* $Car(\bigcup E_i) = \sum_{k=1}^{n}(\sum_{1\leqslant i_1<\dots i_k}(-1)^{k+1}Card(A_{i_1}\cap\dots\cap A_{i_k}))$

On a le pendant au niveau des mesures.

Proposition 6. $\mu(\bigcup E_i)) = \sum_{k=1}^{n}(\sum_{1\leqslant i_1<\dots i_k}(-1)^{k+1}\mu(A_{i_1}\cap\dots\cap A_{i_k}))$

Application 1. *Cf cottrel. Un monsieur distrait écrit n lettres différentes à n personnes différentes et ferme les enveloppes avant d'avoir écirt les adresses, qu'il inscrit ensuite au hasard. La probabilité qu'un destinataire au moins recoive la lettre qui lui est destinée est $\sum -1^n/n!$ (donc autour de $1 - e^{-1} = 0.63$ à 10^{-2} près pour $n \geqslant 6$).*

Application 2. *On lance r balles dans n cases. La probabilité qu'aucune case soit vide est,euh... compliqué.*

Application 3. *La probabilité pour que deux entiers soient premiers entre eux est $6/\pi^2$.*

Application 4. *On appelle nombre de dérangements noté D_k le nombre de permutations d'un ensemble à k éléments n'admettant aucun point fixe. La formule du crible permet assez rapidement de conclure que $D_k = n!\sum_0^n(-1)^k/k!$*

Application 5. *Nombre de surjections d'u nensemble à n éléments dans un ensemble à k éléments, notée $S(n,k)$ vaut $\sum_{l=0}^{k}\left(\begin{pmatrix} f \\ l \end{pmatrix}(-1)^l(k-l)^n\right)$.*

1.2 Arrangements,permutations

Définition 1. *On appelle arrangement p à p d'un ensemble à m éléments tout sous-ensemble rangé contenant p éléments. noté A_m^p*

Théorème 1. $A_m^p = (m-p)!/p!$

Définition 2. *On appelle permutation tout ensemble rangé contenant n éléments.*

Théorème 2. *Nombre de permutations $= n!$.*

1.3 Combinaisons,binôme de Newton

Définition 3. *On appelle combinaison p à pde m élements tout sous-ensemble à p éléments, noté* C_m^p

Proposition 7. *Triangle de Pascal:* $C_m^p = C_{m-1}^p + C_{m-1}^{p-1}$

Proposition 8. $C_m^p = m!/(p!(m-p)!)$

Corollaire 1. *Le produit de p entiers consécutifs est divisible par le produit des p premiers entiers.*

D'autres relations vérifiées par les coefficients du binôme.

Proposition 9.
1. $\sum_i C_n^i = 2n$.
2. *en écrivant* $x^n = ((x+1)-x)^n$, *on obtient* $C_n^p C_p^k = C_n^k C_{n-k}^{p-k} = C_n^{n-p+k} C_{n-p+k}^k$.
3. $C_{m+1}^{p+1} = C_m p + \ldots + C_p^p$.

Application 6 (binôme de Newton)**.** *On considère un anneau A, ainsi que deux éléments A et B de l'anneau qui commutent. Alors* $(A+B)^n = \sum C_n^k A^k B^{n-k}$. *On a aussi la formule du binôme de Newton généralisée* $(A_1 + \ldots + A_p)^n = \sum_{n_1+\ldots+n_p=n} p!/(n_1! \ldots n_p!) a_1^{n_1} \ldots a_p^{n_p}$

Application 7. *Application au calcul de progressions de sommes de la forme* $S_n = a^\alpha + \ldots + l^\alpha + \ldots$ *(Ramis page 94)*
On écrit $(a_j + r)^m = \sum c_m^i a_j^{m-i} i r^i$, *puis on fait la somme sur j.* $\sum (a_j + r)^m = \sum_i \sum_j c_m^i a_j^{m-i} r^i$. *Mais le terme de gauche* $(a_j + r)^m$ *se simplifie avec le terme de droite compte tenu de la relation* $a_{j+1} = r + a_j$. *Donc* $(a_n + r)^m = \sum_{i=1}^m \sum_j c_m^i a_j^{m-i} r^{m-i}$. *On appelle* S_i *la somme des termes à la puissance i. On obtient* $(a_n + r)^m = a_1^m + \sum_{i=1}^m S_{m-i} C_m^i r^i$, *et ce ci permet de calculer de proche en proche les* S_i. $S_0 = n$. $(n+1)^2 = 1^2 + 2 * S_1 + S_0 = 1 + 2S_1 + n$, *ce qui implique la formule pour* S_1. $(n+1)^3 = 1 + 3 * S_2 + 3 * S_1 + n$. *Et ainsi de suite.*

Définition 4. *Combinaison avec répétition de m éléments p à p = on choisit p éléments pas forcément distincts (on peut choisir le même p fois). Notation:* Γ_m^p.

Proposition 10. $p\Gamma_m^p = m\Gamma_m^{p-1} + (p-1)\Gamma_m^{p-1}$

On en déduit

Théorème 3. $\Gamma_m^p = C_{m+p-1}^m$.

Application 8. *Le nombre de termes du polynôme homogène de degré p à m indetermineées. On en déduit* $\Gamma_{m+1}^p = \gamma_m^p + \ldots + \gamma_m^1 + 1$.

1.4 Partitions D'un entier

Définition 5. *Partitions d'un entier = nombre de manière d'écrire n comme sommes d'entiers. Noté p(n).*

Théorème 4. $\sum p(n) X^n = \prod 1/(1-X^i)$.

Application 9. *Nombre de façons de payer 100 euros avec des pieces de 1 euros, 2 euros et un billet de 5 euros : on cherche la valeur de* $u_1 00$ *dans le DSE de* $((1-x)(1-x)^2(1-x^5))^{-1}$.

Application 10. *On se place dans un corps algébriquement clos et on considère le nombre de classes de similitudes d'endomorphismes ayant un polynôme caractéristique donné, noté* $Sim(P)$. *Soit* $j_1, \ldots j_r$ *la taille des blocs de Jordan. Alors comme les réduites de Jordan caractérisent les classes de similitude, on a* $Sim(P) = \sum p(j_i)$.

2 Raisonnements combinatoires basés sur le principe des tiroirs ou le double décompte

2.1 Principe des tiroirs et applications

Théorème 5. *Si r objets (ou une infinité d'objets) sont placés dans n boîtes avec $n < r$ alors il y a au moins deux objets dans la même boîte.*

Application 11. *Choisissons $n+1$ nombres parmi $\{1, 2, \ldots, 2n\}$. Il y en a au moins deux qui sont premiers entre eux. Il y en a au moins deux tel que l'un divise l'autre*

Application 12. *Si l'on se donne $mn+1$ nombres réels distincts, alors il existe une suite strictement croissante de taille $n+1$, ou une suite strictement décroissante de taille $m+1$, ou les deux à la fois*

Application 13. *Si l'on considère n nombres entiers distincts ou non, alors on peut toujours trouver un ensemble consécutif de ses nombres qui est un multiple de n.*

Application 14. *Approximation d'un réel: $|x - p/q| < 1/q^2$*

Application 15. *Sujet analyse 2009: o nen déduit le théorème de relèvemetn continu des fonctions complexes.*

2.2 Double décompte et applications

Théorème 6. *On considère deux ensembles finis L et C, et un sous-ensemble $S \subset L \times C$. si $(p, q) \in S$ on dit que p et q sont incidents. $l_p =$ les q tq (p, q) incidents, de même pour c_q. Alors $|S| = \sum_{p \in L} l_p = \sum q \in C c_q$.*

Définition 6. *Matrice d'incidence $A = (1_{(i,j) \in S})$.*

Application 16. *On considère $L = C$ l'ensemble des n premiers ensembles et $S := \{(i, j), i|j\}$. Alors le nombre de diviseur de j, noté $t(j)$, est exactement le nombre de 1 dans la colonne numéro j. Il est remarquable que la moyenne $\bar{t}$ est telle que $ln(n) - 1 < \bar{t}(n) < ln(n) + 1$. Donc $\bar{t}$ est équivalent à $ln(n)$ quand t tend vers ∞.*

Définition 7. *Graphe fini simple = couple (V, E, φ) où V est l'ensemble des sommets fini et E l'ensemble des arêtes fini, et $\varphi : E \to V \times V$ qui à chaque arête associe deux sommets distincts et la fonction est de plus injective.*

Définition 8. *Degré d'un sommet: nombre d'arêtes qui passent par ce sommet, noté $d(v)$.*

Un double décompte permet de démontrer le théorème suivant.

Théorème 7. $\sum_{v \in V} d(v) = 2E$

Définition 9. *Graphe dual: on place un point à l'intérieur de chaque face du graphe, et un point à l'extérieur du graphe, et on rejoint les points qui correspondent à des face adjacentes. Ce n'est plus un graphe simple en général.*

Lemme 1 (Spencer)**.** *On considère un grand triangle que l'on triangule. On colorie les sommets du graphe obtenu avec 3 couleurs de manière à ce que les 3 sommets soient de trois couleurs différentes et les sommets sur un côté du grand triangle ne sont coloriés que par les deux couleurs des sommets de ce côté. Alors il existe un triangle tricolore, et même il en existe un nombre impair.*

Application 17 (Brouwer)**.** *Toute application continue du disque unité sur lui-même admet un point fixe.*

2.3 Formule de Burnside et applications

Par un double décompte on démontre

Théorème 8. *Soit G un groupe fini agissant sur un ensemble fini X. Soit $g \in G$. on note $fix(g)$ l'ensemble des points fixes de g pour l'action de G sur X. Alors le nombre d'orbites vaut* $1|G\sum_{g\in G}|fix(G)|$

Application 18. *On se donne 4 perles rouges, 3 perles bleues et 2 perles jaunes. On peut à l'aide de ses éléments fabriquer 76 colliers différents. Si on se donne 4 perles rouges, 6 perles bleues et 4 perles jaunes, on peut fabriquer 7575 colliers différents.*

Application 19. *Le nombre de colorations d'un collier à n perles avec m couleurs est* $1/n\sum_{d|n}\varphi(d)m^{n/d}$ *(seules les rotations du collier sont considérées ici)*

Application 20. *Il y a 57 manières de colorier le cube avec 3 couleurs (ou moins) . Il y a* $1/24*(|C|^6+6*|C|^3+8*|C|^2+6*|C|^3+3*|C|^4)$ *manières de colorier le cube avec C couleurs (ou moins).*

Faire de même avec tétraèdre et icosaèdre en utilisant la formule $1/g\sum|C|^{\gamma(g)}$ où $\gamma(g)$ designe le nombre de cycles de g dans sa d´ecomposition en cycles a supports disjoints

Définition 10. *On appelle pôle d'un rotation u différente de l'identité l'intersection de l'axe de U et de la sphère unité. C'est un ensemble à n éléments. Soit G un sous-groupe fini de $SO(3,R)$ non trivial de cardinal n . On note X l'ensemble des pôles des éléments de G privé de l'identité. X est un ensemble de cardinal au moins 2 et inférieur à* $2(n-1)$

Proposition 11. *G agit sur X de la manière évidente, ie $g.x = g(x)$.*

En utilisant cette action, la formule des classes et la formule de Burnside, on démontre

Théorème 9. *Les sous-groupes finis de $SO(3,R)$ sont soient des groupes cycliques, soient isomorphes à un groupe diédral, soit isomorphes à un des trois groupes d'isométries des solides platoniciens.*

Application 21 (Fermat [1][page 170)**.** *n^p est congru à n modulo p.*

3 Autres méthodes combinatoires

3.1 Utilisation des séries génératrices

Définition 11. *On considère une suite de cardinaux A_n qu'on aimerait bien calculer; On lui associe deux séries formelles suivantes appelées série entière génératrice et série exponentielle génératrice :* $\sum_{n=0}^{\infty}A_nX^n$ *et* $\sum_{n=0}^{\infty}A_n/n!X^n$

Proposition 12. *L'ensemble des séries génératrices est muni d'une structure d'algèbre pour (+,.,*) où * est la convolution. De plus c'est un espace ultramétrique pour une métrique que je ne donne pas ici.*

Application 22. *Retour sur les dérangements. Ils vérifient* $\sum C_n^kD_k = n!$. *On considère la série génératrice* $\sum D_k/k!X^k$. *On montre que son rayon de convergence est plus grand que* 1. *On montre que la série génératrice vaut* $e-z/(1-z)$ *et on en déduit que D_k est la partie entière de* $k!/e+1/2$, *et donc qu'asymptotiquement D_k est équivalent à* $k!/e$.

Application 23. *Nombre de Bell B_n= nombre de partitions d'un ensemble à n éléments. Ils vérifient* $B_{n+1} = \sum_{k=0}^{n}C_n^kB_k$. *On considère la série génératrice* $\sum b_n/n!X^n$. *On montre qu'elle vérifie une équation différentielle du type* $T' = e^XT$. *On monre à l'aide de ceci que* $B_n = \sum_1^n S(n,k)$.

Application 24. *Nombre de Catalan: en considérant encore la série génératrice entière ce coup-ci, on obtient que le nombre de produits différents est* C_{2n-2}^{n-1}/n.

3.2 Utilisation des formules d'inversion

Définition 12. *La fonction de Möbius est définie de N* dans -1, 0, 1. Si n est un nombre entier, son image par la fonction est généralement noté $\mu(n)$, elle est nulle si n est divisible par un carré parfait différent de 1, vaut 1 si n est le produit d'un nombre pair de nombres premiers distincts et -1 sinon.*

Proposition 13. *C'est une fonction multiplicative. De plus, $\sum_d^n \mu(d) = \delta_{n,1}$.*

Corollaire 2. *On considère une suite de nombres complexes a_n, et $b_n := \sum_{d|n} a_d$. Alors $a_n = \sum_{d|n} \mu(n/d)g(d)$.*

Application 25. *On retrouve le nombre de surjections avec la formule d'inversion (car $\sum_{k=0}^n (-1)^k C_n^k C_{p-k}^{n-k} =$ 1 si $p = 0$, 1 sinon, et on utilise l'inversion)*

Application 26. *Notons $I(n,q)$ le nombre de polynômes unitaires irréductibles de degré n sur Fq. Alors, on a $I(n,q) = 1/n \sum_{d|n} \mu(n|d)q^d$.*

References

[1] Combes