⚠ On reste ds le cadre d'ensembles finis.

NOM : AUFORT **Prénom :** William **Jury :**

Algèbre ← Entourez l'épreuve → **Analyse**

Sujet choisi : 190 : Méthodes combinatoires, problèmes de dénombrement

Autre sujet :

I Cardinalité : les fondamentaux

a) Notion de Cardinal, Premiers exemples

Déf 1 Soit E un ensemble. Si E contient un nombre fini d'éléments, on dit que E est fini et on appelle cardinal de E, noté Card(E) ou $|E|$, le nombre d'éléments de E.

Prop 2 Si $f : E \to F$ finis est bijective alors Card E = Card F.

+ injec° et surjec°

$A \subset B \Rightarrow$ Card A $\leq$ Card B +

Remarque 3 C'est la base du dénombrement : on cherche souvent à établir une bijection de l'ensemble à dénombrer vers un ensemble dont le cardinal est connu ou calculable. (inégalités)

Prop 4 : Soient E et F deux ensembles finis. Alors
- $\text{Card}(E \times F) = \text{Card } E \times \text{Card } F$
- $\text{Card}(\mathcal{F}(E,F)) = |F|^{|E|}$
- $\text{Card}(\mathcal{P}(E)) = 2^{\text{Card}(E)}$

fmle du binôme $2^n = \sum \binom{n}{k}$

b) Coefficients binomiaux

Déf 5 : Si $n \geq p \geq 0$, on pose $\binom{n}{p} = \frac{n!}{p!(n-p)!}$

Prop 6 : Le nombre de combinaisons à p éléments d'un ensemble à n éléments est $\binom{n}{p}$. Le nombre d'injections (ou arrangements) est $\binom{n}{p} p! = \frac{n!}{(n-p)!}$. Le nombre de permutations (ou bijections) d'un ensemble à n éléments est $n!$

Prop 7 : $n! \underset{+\infty}{\sim} \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ (Formule de Stirling)

Ex 8 : Combien forme-t-on de triangles en traçant dans le plan n droites en position générale ?

Ex 9 : Le nombre de couples de parties de E dont l'union recouvre E est $3^{|E|}$.

Remarque 10 Trouver le nombre de surjections de E dans F est plus difficile (voir Ex 32,5)

c) Méthodes élémentaires :

Comme dit dans la remarque 3, on se ramène via des bijections à des cardinaux "plus simples".

Ex 11 $\text{Card}(GL_n(\mathbb{Z}/p\mathbb{Z})) = \prod_{i=0}^{n} (p^n - p^i)$.

Ex 12 On place 100 entiers relatifs de somme 1 sur un cercle. Quel est le nombre de suites de nombres qui se suivent sur le cercle de somme strictement positive ?

Remarque 13 : Une autre méthode élémentaire consiste à chercher une relation de récurrence faisant intervenir la quantité à dénombrer.

Ex 14 : Soit u_n le nombre de pavage d'un damier $2 \times n$ par des dominos 2×1. On a $u_{n+2} = u_{n+1} + u_n$, et on peut trouver u_n ensuite

Ex 15 : Nombre de chemins reliant deux sommets d'un cube de l'espace via n arêtes ?

Remarque 16 Les récurrences linéaires peuvent facilement résolues. Dans le cas contraire, il y a quelques méthodes qui peuvent aboutir.

Manque : Partition de n = pb difficile qui intéresse bcp de gens en combi

1/4

II Méthodes analytiques

a) Formule du Crible

Prop 17 (Formule du Crible) Si $U_1, \dots, U_k$ sont k ensembles finis, alors
$$\mathrm{Card}\left(\bigcup_{i=1}^{k} U_i\right) = \sum_{\substack{I \subset [\![1,k]\!] \\ I \neq \emptyset}} (-1)^{1+\mathrm{Card}\, I}\, \mathrm{Card}\left(\bigcap_{j \in I} U_j\right)$$

Appli 18 Le nombre de permutations de $\mathfrak{S}_n$ sans point fixe est $n!\left(\sum_{k=0}^{n} \frac{(-1)^k}{k!}\right) = D_n$

Appli 19 La probabilité que 2 nombres choisis aléatoirement unif. dans $[\![1,n]\!]^2$ soient premiers entre eux est $r_n = \frac{1}{n^2}\sum_{d=1}^{n} \mu(d) E\left(\frac{n}{d}\right)^2$, où E est la partie entière, μ est la fonction de Mobius (voir déf 26)

b) Récurrences et séries génératrices

Déf 20 Soit $(a_n) \in \mathbb{R}^{\mathbb{N}}$. On appelle :
- série génératrice de $(a_n)_{n\in\mathbb{N}}$ la série $\sum_{n=0}^{+\infty} a_n z^n$
- série génératrice exponentielle de $(a_n)_{n\in\mathbb{N}}$ la série $\sum_{n=0}^{+\infty} \frac{a_n}{n!} z^n$.

Idée 21 : L'utilisation des séries génératrices et des opérations sur les séries (produit notamment) peut permettre d'"inverser" une relation de récurrence vérifiée par (a_n) pour obtenir a_n.

Appli 22 La série génératrice de $(D_n)_{n\in\mathbb{N}}$ (voir exemple 18) est $\sum_{n=0}^{+\infty} \frac{D_n}{n!} z^n = \frac{e^{-z}}{1-z}$.

Remarque 23 Ces séries peuvent être vues comme des séries entières ou formelles (dans ce cas on ne s'occupe pas du rayon de convergence).

Appli 23 Le nombre de parenthésages d'un produit matriciel $M_1 \dots M_n$ est $C_n = \frac{1}{n}\binom{2n-2}{n-1}$ (nombre de Catalan)

Appli 24 Le nombre de partitions de $[\![1,n]\!]$, noté B_n, vérifie : $\sum_{n=0}^{+\infty} \frac{B_n}{n!} z^n = e^{e^z - 1}$ pour $z \in]-R;R[$, où R est le RCV de la série entière $(R>0)$.

c) Formules d'inversion

Idée 25 Dans certaines situations, des formules d'inversion (cf idée 21) existent.

① Inversion de Mobius

Déf 26 On appelle fonction de Mobius la fonction $\mu : \mathbb{N}^* \longrightarrow \{0,1,-1\}$
$$n \longmapsto 0 \text{ si } n \text{ a un facteur carré}$$
$$p_1 \dots p_r \longmapsto (-1)^r \ (p_i) \text{ premiers distincts}$$

Lemme 27 :
- μ est multiplicative : si $m \wedge n = 1$, alors $\mu(mn) = \mu(m)\mu(n)$
- $\sum_{d|n} \mu(d) = 0$ si $n > 1$

Théorème 28 (Inversion de Mobius)
Si $a_n = \sum_{d|n} b_d$, alors $b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d$.

Appli 29 Soit $I(n,q)$ le nombre de polynômes de $\mathbb{F}_q[X]$ de degré n, unitaires et irréductibles. On a $I(n,q) = \frac{1}{n}\sum_{d|n} \mu(n/d) q^d$. De plus $I(n,q) \underset{n\to+\infty}{\sim} \frac{q^n}{n}$. DEV1

Rem 29,5 On peut montrer par la même occasion que $I(n,q) > 0$, si q est premier on peut reconstruire les corps finis.

↳ non car on utilise l'$\exists$ce d'un corps fini à q élts dans la dem du 29.

② Inversion de Pascal

Lemme 30 $\sum_{k=0}^{p} (-1)^k \binom{n}{k}\binom{n-k}{p-k} = \begin{cases} 1 & \text{si } p = 0 \\ 0 & \text{si } p \geq 1. \end{cases}$

Théorème 31 (Inversion de Pascal) : Si $a_n = \sum_{k=0}^{n} \binom{n}{k} b_k$, alors $b_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} a_{n-k}$.

Ex 32 : À l'aide de l'inversion de Pascal, on peut retrouver le résultat de l'appli 18.

Ex 32,5 : Nombre de surjections de $[\![1,n]\!]$ dans $[\![1,p]\!]$.

III Interactions et applications à d'autres domaines

a) Groupes

Remarque 33 La prop 2 s'étend aux morphismes de groupes : on peut calculer des cardinaux via des isomorphismes, et inversement à l'aide des cardinaux conclure qu'un morphisme est bijectif.

Ex 34 : Si $f \in \mathrm{Hom}(G,G')$, alors $G/\mathrm{Ker} f \simeq \mathrm{Im} f$. On a donc $|\mathrm{Ker} f| \times |\mathrm{Im} f| = |G|$.

Appli 35 : $\mathrm{Card}(SL_n(\mathbb{F}_q)) = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i)$

Ex 36 : Si $p > 2$, $\bar{x}$ est un carré de $\mathbb{Z}/p\mathbb{Z}$ si et seulement si $\bar{x}^{\frac{p-1}{2}} = 1$.

Théorème 37 (Équation des classes) Soit $G \curvearrowright E$ finis, $O_1 \dots O_k$ les orbites pour cette action, $x_i \in O_i$. Alors $\mathrm{Card}\,|E| = \sum_{i=1}^{k} \mathrm{Card}(O_i)$ et $\mathrm{Card}(O_i) = \frac{|G|}{|\mathrm{Stab}(x_i)|}$

Combo

Théorème 38 (Formule de Burnside) Sous les mêmes hypothèses, le nombre d'orbites K est
$$K = \frac{1}{|G|}\sum_{g\in G} |fix(g)| \quad \text{où } fix(g) = \{x\in E,\ g.x = x\}$$

Appli 39 : Combien de colliers différents peut-on faire avec 4 perles bleues, 3 perles blanches et 2 perles rouges ?

Appli 40 Le centre d'un p-groupe est non trivial.

Remarque 41 Le dénombrement intervient aussi beaucoup dans la théorie des p-Sylows :

Théorème 42 (Sylow) Si $|G| = p^\alpha m$, $p \nmid m$ alors
- G contient au moins un p-Sylow (ie un sous-groupe de cardinal p^α)
- les p-Sylow de G sont conjugués, leur nombre k divise donc m
- on a aussi $K \equiv 1 \mod p$.

b) Graphes

Déf 43 Un graphe G est la donnée d'un ensemble V de sommets et d'un ensemble $E \subset V\times V$ d'arêtes. Le degré d'un sommet $v\in V$ est $Card\{u\in V, (v,u)\in E\}$

Prop 44 $\sum_{v\in V} \deg v = 2|E|$

Appli 45 : Une famille de transpositions qui engendre $\mathfrak{S}_n$ a au moins $n-1$ éléments.

Déf 46 Supposons $V = \{1,\dots,n\}$. La matrice d'adjacence de G est une matrice $M\in M_n(\{0,1\})$ où $m_{ij} = 1 \Leftrightarrow (i,j)\in E$.

Appli 47 Le calcul de M^n nous donne le nombre de chemins allant d'un sommet i à un sommet j pour tous (i,j). On peut alors retrouver le résultat de 15, mais avec une matrice plus grande...

Ex 48 : Si G ne contient pas de cycle de longueur 4 alors
$$|E| \le \left\lfloor \tfrac{n}{4}\left(1+\sqrt{4n-3}\right)\right\rfloor \text{ où } n = |V|.$$

c) Probabilités

1) Lien proba/dénombrement

Remarque 49 Le dénombrement intervient naturellement en proba sur des ensembles finis (cf Appli 19) : Sur un espace probabilisé $(\Omega, \mathcal{P}(\Omega), \mathbb{P})$ où Ω fini et $\mathbb{P}$ est la proba uniforme sur Ω, on a
$$\mathbb{P}(A) = Card A / Card\ \Omega.$$
Cette relation permet de passer d'une proba à un cardinal, et réciproquement.

Ex 50 : Dans une marche aléatoire sur $\mathbb{Z}$, la probabilité de revenir à un état x, partant de x, au bout de $2n$ étapes est $\frac{1}{2^{2n}}\binom{2n}{n}$. La théorie des chaînes de Markov dit alors que tous les états sont récurrents.

Ex 51 : En étudiant la fonction génératrice d'une variable aléatoire ($\mathbb{E}(t^X)$) bien choisie, on peut obtenir le nombre de nombres à 6 chiffres $\overline{abcdef}^{10}$ tels que $a+b+c = d+e+f$. (a peut être nul, etc...)

Rem 52 : Il faut une v.a. X positive pour que $\mathbb{E}(t^X)$ soit défini.

2) Existence combinatoire et méthode probabiliste

Idée 53 Si $\mathbb{P}(A)>0$, alors $\exists\omega\in\Omega$ satisfaisant Ω. De même, si X est une variable aléatoire telle que $\mathbb{E}(X)=a$, alors $\exists\omega\in\Omega$ tel que $X(\omega)\ge a$. En calculant ces quantités, on peut démontrer l'existence d'objets vérifiant certaines propriétés, qui est une branche importante de la combinatoire.

Ex 54 : Un tournoi est un graphe orienté complet ie $(x,y)\in E$ ou $(y,x)\in E$ $\forall x,y\in V$. Soit $n = |V|$. Alors, si $k\in\mathbb{N}$ est tel que $\binom{n}{k}\left(1-\frac{1}{2^k}\right)^{n-k} < 1$, alors il existe un tournoi tel que pour tout sous ensemble à k joueurs, il existe un autre joueur qui les bat tous.

Ex 55 : Dans $\mathbb{R}^n$ euclidien si $v_1 \dots v_n$ sont des vecteurs de norme 1, alors on peut les mettre "bout à bout" de manière à obtenir un vecteur de norme $\ge \sqrt{n}$, autrement dit $\exists(\varepsilon_1 \dots \varepsilon_n)\in\{-1;1\}^n$, $\|\sum_{i=1}^n \varepsilon_i v_i\| \ge \sqrt{n}$ (voir annexe)

Ex 56 Si $A\in\mathcal{M}_n(\{-1;1\})$, alors il existe $(x,y)\in\{-1;1\}^n$ tels que
$$\sum_{i,j} a_{ij} x_i y_j \ge \left(\sqrt{\tfrac{2}{\pi}} + o(1)\right) n^{3/2}.$$

Appli 57 Jeu de Berlekamp (voir annexe)

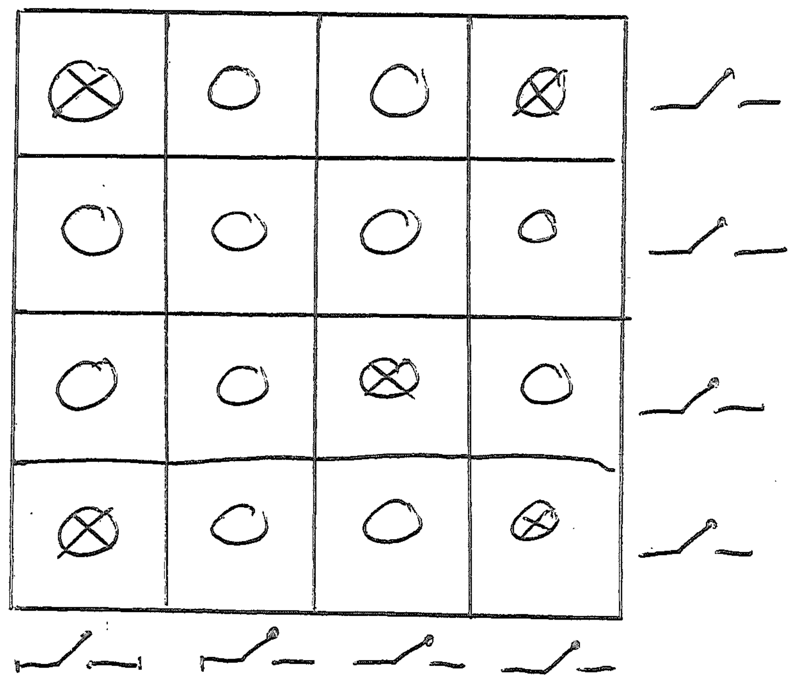
DEV 2

original :)

Remarque 58 : Ce genre de méthodes s'applique à beaucoup de domaines (graphes, algèbre linéaire, géométrie...)

Annexe. Jeu de Berlekamp

On place sur une matrice $n \times n$ des ampoules initialement allumées ou éteintes. Sur chaque ligne et chaque colonne, un interrupteur permet de changer l'état de toutes les ampoules sur la-dite ligne/colonne. Le résultat de la proposition 56 nous permet d'en déduire qu'à partir de toute configuration initiale on peut arriver à allumer $\frac{n^2}{2} + \frac{1}{\sqrt{2\pi}} n^{3/2} + o(n^{3/2})$ ampoules en utilisant les interrupteurs.



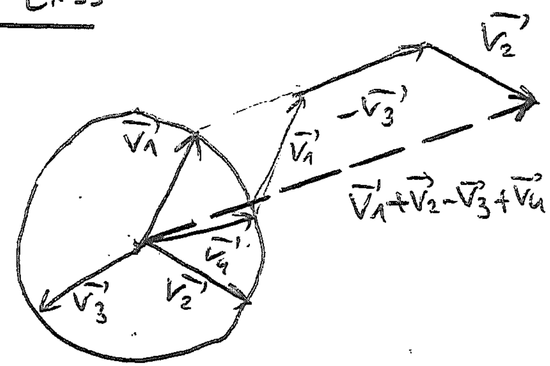
Références

Les principales:
- FGN Algèbre 1 : pour l'essentiel de Ic et II et l'appli 45
- Cottrell, Duhamel : Ia, Ib, III c ①.
- Perrin et Combes pour III a
- Alon, Spencer The probabilistic method pour III c ②.

Quelques exemples viennent de :
- Proofs from the book (Ex 48) – Giorgi, Théories math. pr l'agreg (Ex 8 et 9)
- Initiation aux probabilités et aux chaînes de Markov (Ex 51)

III b (graphes) sans référence (sauf Appli 45 / Ex 48), mais ça doit être dans le Cormen (Introduction to algorithms), mais bon c'est simple à retenir...

Annexe : Ex 55



- **Oraux 2**

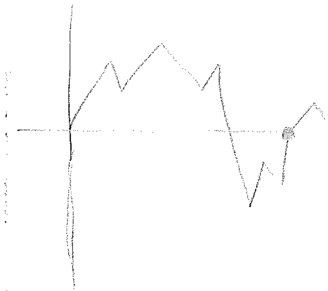
  – Ne pas faire l'appli et détailler plus les calculs

- **Autres**

  – Fmle du chef $\binom{n}{k} k = \binom{n-1}{k-1} n$

  – Dobble

  – Marche aléatoire sur $\mathbb{Z}$ (appli de Stirling)



(ex 50)

$$\mathbb{P}(\quad) = \binom{2N}{N} \frac{1}{2^{2N}} \sim \cdots$$

  – Lemme des tiroirs
    Enigme des personnes qui se serrent la main.

  – paradoxe des anniversaires (cf. Foata & Fuchs)

- **Commentaires**

  – Justifier Stirling

  – lemme des tiroirs

  – lemme des bergers $\rightarrow$ + gnal : si on a une partition, ... ($\swarrow$ implt)

  – séries génératrices (++), réfléchir si les série formelle ou série entière

  – fmle du binome / fmle du multi-nome

  – géom sur les corps finis possible $|\mathbb{P}^n(\mathbb{F}_q)| = \frac{q^{n+1}-1}{q-1}$

    $\mathbb{F}_q^{\,n} \sqcup \mathbb{P}^{n-1}(\mathbb{F}_q) = q^n + |\mathbb{P}^{n-1}(\mathbb{F}_q)| = q^n + q^{n-1} + \dots + 1$

    Morale : compter des choses n'est pas forcément le but, pfs on montre une formule en comptant la m̂ chose de plusieurs manières

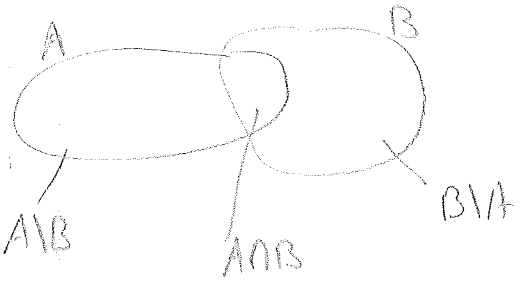
  – dénombrement d'alg linéaire, tableaux de Young, cf Caldero

  – Bible = analytic combinatorics, Flajolet & Sedgewick (lire l'intro)

  – Sommer sur des entiers ou sur pas des entiers (eg. arbres ...) fmle de Wick.

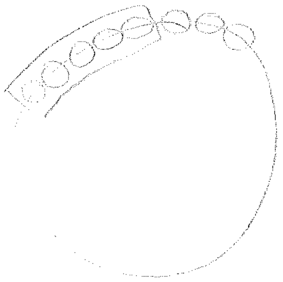
• Questions

- Ex 9 ? $(A,B) \in \mathcal{P}(E)^2$, $A \cup B = E$



3 couleurs.

- Ex 12 ?

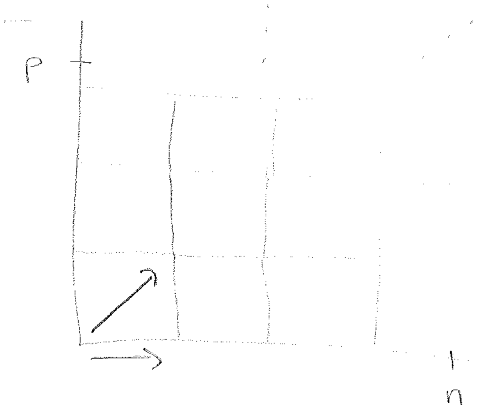


$a_1 + \dots + a_{100} = 1$

$$\frac{100 \times 99}{2} = 1 + 2\,\mathrm{card}(E)$$

- Appli 12 ?

• Exercices



|| nombre de chemins de $(0,0)$ à (n,p) ?

↳ * si $p > n$: 0

* p déplacements NE

$n-p$ ... E.

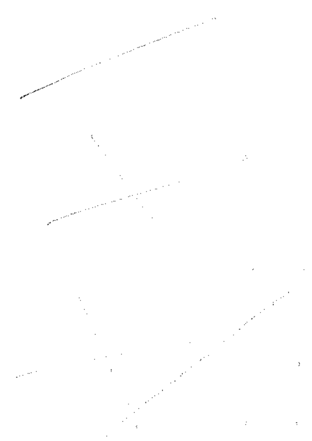
↳ $\binom{n}{p} = \binom{n}{n-p}$

- || Oh (?). Nombre de classes de similitude d'endo. nilpotents ?

↳ Utiliser Jordan : ds une certaine base $Mat_{\mathcal{B}}\, u = \begin{pmatrix} 0 & 1 & \\ & 0 & \ddots \\ & & \ddots \end{pmatrix}$

- || n dtes en positions générique

|| nbre de composantes connexes de le compl ? C_n



↳ * $n = 1$: $C_n = 2$

* $n = 2$: $C_n = 4$

* $n = 3$: $C_n = 7$

* n dtes. n intersec° $C_{n+1} = C_n + 2 + (n-1) = C_n + n + 1$

- || tirer deux cartes uniformément parmi 52. proba d'une paire ?

↳ $\mathbb{P}(\text{paire}) = \frac{3}{51} = \frac{1}{17}$

| Séries finies
| peut se mettre ds le plan

- || $x + 2y = n$. $n \in \mathbb{N}$. $(x,y) \in \mathbb{N}^2$ $p_n = \#$ sol° de cette eq°

↳ $f(z) = \sum_{n=0}^{+\infty} p_n z^n$ $\left(\sum_{n=0}^{+\infty} z^n\right)\left(\sum_{p=0}^{+\infty} z^{2p}\right) = \sum_{k=0}^{+\infty} p_k z^k$

$\frac{1}{1-z}$ $\frac{1}{1-z^2}$

$$\frac{1}{(1-z)(1-z^2)} = \frac{1}{(1-z)^2(1+z)} = \frac{a}{1+z} + \frac{b}{1-z} + \frac{c}{(1-z)^2}$$

$a = 1/4$

$c = 1/2$

$b = 1/4$ (eq. éval en 0).

$$= \frac{1}{4}\,\frac{1}{1+z} + \frac{1}{4}\,\frac{1}{1-z} + \frac{1}{2}\underbrace{\left(\frac{1}{(1-z)^2}\right)}_{\left(\frac{1}{(1-z)}\right)'}$$

(4

$$= \frac{1}{4}\sum_{k=0}^{\infty}(-z)^k + \frac{1}{4}\sum_{k=0}^{\infty} z^k + \frac{1}{2}\sum_{k=0}^{\infty}(n+1)z^n$$

$$p_k = \frac{\left((-1)^n + 1\right)}{4} + \frac{1}{2}(n+1)$$

– || nombre de chemins allant de $(0,0)$ à (n,s) ?

H = # déplacements ht
B = # — bas

$\begin{cases} H+B = n \\ H-B = s \end{cases}$

$\longrightarrow H = \frac{n+s}{2}$

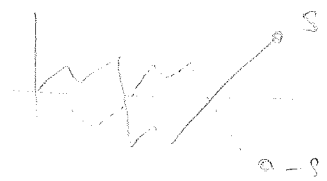
$B = \frac{n-s}{2}$

0 si $n+s$ impair

$\binom{n}{\frac{n+s}{2}}$ si $n+s$ pair

|| nombre de chemins allant de $(0,0)$ à (n,s) sans passer par $(0,k)$?

→ principe de sym. : à tt chemin de $0 \to s$ touchant 0, on associe un chemin de $0 \to -s$ en symmétrisant :



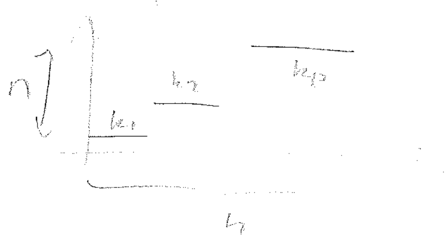
↙ cf Foata, Fuchs
(Chap. Proba discrètes)

appli : thm du scrutin

chemin de dick ⟷ nbres bien parenthésés ⟷ arbres enracinés
= nbre de Catalan

– || $f : \mathbb{R}^n \to \mathbb{R}$ nbres de dériv. partielles d'ordre k ? (permuta°ok)

$$D^k f : \frac{\partial^k f}{\partial x_1 \dots \partial x_n}$$



$$\#\left\{ (k_1, \dots, k_n) \in \{1, \dots, k\}^n \;\middle|\; \sum_{i=1}^{n} k_i = k \right\}$$

$$\| \text{rlq} = \binom{n+k-1}{n-1}$$

(| | |) ‡ | | ‡ | ‡ | | |)

← $n+k-1$ batons

on en choisit $n-1$

→ n paquets, somme $= k$