Chapitre 4

Dénombrement

4.1. Fonctions génératrices

4.1.1. Séries formelles

Supposons qu'on ait un problème dont la solution soit une suite de nombres $a_0, a_1, \ldots$. On aimerait « savoir » de quelle suite il s'agit. Que veut-on dire par là ? Une réponse possible est d'obtenir une formule close pour les a_n. Par exemple, si on trouve que $a_n = 3n + 1$, on serait satisfait de la réponse. Néanmoins, il n'est pas toujours possible de trouver une forme close. Par exemple pour la suite $2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$ où a_n est le $n^{\text{ème}}$ nombre premier, il ne serait pas raisonnable d'espérer une expression close. Ainsi, même si une formule simple pour les a_n n'existe pas toujours, il peut être possible de donner une formule pour la somme formelle : $\sum_{n\geq 1} a_n x^n$. Une telle expression est une *série formelle*.

Définition 4.1. Une *série formelle* P est une application f de $\mathbb{N}$ dans $\mathbb{R}$. On représente une série formelle par l'expression $P = \sum_{n\geq 0} f(n)x^n$. Les séries formelles peuvent être additionnées et multipliées à l'aide des règles suivantes :

$$\begin{aligned} \sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n &:= \sum_{n\geq 0} (a_n + b_n) x^n \\ \left(\sum_{n\geq 0} a_n x^n\right) \cdot \left(\sum_{n\geq 0} b_n x^n\right) &:= \sum_{n\geq 0} \left(\sum_{i+j=n} a_i b_j\right) x^n. \end{aligned}$$

L'ensemble des séries formelles est noté $\mathbb{R}[[x]]$.

L'adjectif « formel » veut dire qu'on ne s'intéresse pas à la convergence d'une telle série. On s'intéresse uniquement aux propriétés combinatoires des coefficients d'une telle série.

Théorème 4.2. *L'ensemble $\mathbb{R}[[x]]$ muni des opérations d'addition et de multiplication est un anneau. Les séries formelles $0 = \sum_{n\geq 0} 0x^n$ et $1 = 1 + \sum_{n\geq 1} 0x^n$ sont respectivement les éléments neutres de l'addition et de la multiplication. Un élément $\sum_{n\geq 0} a_n x^n$ est inversible dans cet anneau si et seulement si $a_0 \neq 0$.*

Démonstration. La seule assertion difficile est l'inversibilité. Supposons que $P = \sum_{n\geq 0} a_n x^n$. Soit $Q = \sum_{n\geq 0} b_n x^n$. Si $a_0 = 0$, alors le coefficient x^0 de PQ est 0, ainsi on voit que ce produit ne peut jamais valoir 1 et que donc P n'a pas d'inverse pour la multiplication. Inversement, supposons $a_0 \neq 0$. On veut calculer par récurrence les coefficients b_n de Q de telle manière que $PQ = 1$. Le coefficient de x^0 dans PQ est $a_0 b_0$, donc on doit avoir $b_0 = 1/a_0$. Supposons maintenant qu'on ait déjà calculé pour $n \geq 1$ les coefficients $b_0, b_1, \ldots, b_{n-1}$ de telle manière que les coefficients de $x^1, \ldots, x^{n-1}$ dans PQ soient nuls et que le coefficient de x^0 dans ce produit soit 1. Le coefficient de x^n dans ce produit est $a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0$. Pour qu'il soit nul, on doit poser $b_n = -(a_1 b_{n-1} + a_2 b_{n-2} + \cdots + a_n b_0)/a_0$, ce que l'on peut faire car $a_0 \neq 0$ par hypothèse. Cette construction termine la preuve. □

Définition 4.3. Si P est une série formelle et Q est son inverse, alors on écrit $Q = 1/P$. Plus généralement, $Q = T/P$ pour des séries formelles Q, T, P veut dire que $PQ = T$.

Proposition 4.4. *On a les identités suivantes dans* $\mathbb{R}[[x]]$ *:*

(1) $1/(1-x) = \sum_{n\geq 0} x^n$.

(2) *Si* a, b, c, d *sont des nombres réels avec* $a \neq b$*, alors on a*

$$\frac{c+dx}{(1-ax)(1-bx)} = \sum_{n\geq 0} (Aa^n + Bb^n)\, x^n,$$

avec $A = (d+ac)/(a-b)$ *et* $B = c - A$*.*

Démonstration. (1) On a $(1-x)\sum_{n\geq 0} x^n = \sum_{n\geq 0} x^n - \sum_{n\geq 1} x^n = 1$.

(2) Un simple calcul nous montre que

$$\frac{c+dx}{(1-ax)(1-bx)} = \frac{A}{1-ax} + \frac{B}{1-bx}.$$

En appliquant le résultat précédent avec ax et bx à la place de x, on obtient l'affirmation. □

Définition 4.5. Soit $a_0, a_1, a_2, \ldots$ une suite de nombre réels. Alors la série formelle $A := \sum_{n\geq 0} a_n x^n$ est appelée la *fonction génératrice* de cette suite.

On est maintenant en mesure de donner un premier exemple de l'utilisation des fonctions génératrices en obtenant une formule close pour la suite des nombres de Fibonacci.

Théorème 4.6. *Pour* $n \geq 0$*, définissons la suite* F_n *par* $F_0 := 0$*,* $F_1 := 1$*,* $F_n := F_{n-1} + F_{n-2}$ *pour* $n \geq 2$*. alors on a pour tout* n

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Démonstration. Soit $F := \sum_{n\geq 0} F_n x^n$. Comme $F_n - F_{n-1} - F_{n-2} = 0$ pour tout $n \geq 2$, on a

$$F - \sum_{n\geq 1} F_{n-1}x^n - \sum_{n\geq 2} F_{n-2}x^n = F_0 + F_1 x = x.$$

On peut maintenant remarquer que $\sum_{n\geq 1} F_{n-1}x^n = \sum_{n\geq 0} F_n x^{n+1} = xF$. De manière similaire, $\sum_{n\geq 2} F_{n-2}x^n = x^2F$. Ainsi, on a $F(1-x-x^2) = x$, ce qui nous donne

$$F = \frac{x}{1-x-x^2}$$

dans $\mathbb{R}[[x]]$. En utilisant la formule de la proposition 4.4 (2), on obtient le résultat. □

Voici un autre exemple.

Exemple 4.7. Supposons que $a_0, a_1, \ldots$ soit une suite d'entiers avec $a_0 = 0$, et $a_n = 2a_{n-1} + 1$ pour $n \geq 1$. On aimerait trouver une formule close pour a_n. Soit $f := \sum_{n\geq 0} a_n x^n$ la fonction génératrice de cette suite. Alors $f = \sum_{n\geq 1}(2a_{n-1}+1)x^n$. Remarquez que $\sum_{n\geq 1} a_{n-1}x^n = xf$, et que $\sum_{n\geq 1} x^n = 1/(1-x) - 1 = x/(1-x)$, de telle sorte que $f = 2xf + x/(1-x)$. Ou encore $f = x/(1-x)(1-2x)$. En appliquant la proposition 4.4 (2) on en déduit que

$$f = \sum_{n\geq 0}(2^n - 1)x^n,$$

et donc que $a_n = 2^n - 1$ pour $n \geq 0$. ◇

4.1.2. L'opérateur de dérivation

Définition 4.8. L'*opérateur de dérivation* $\partial\colon \mathbb{R}[[x]] \to \mathbb{R}[[x]]$ est définit par $\partial(\sum_{n\geq 0} a_n x^n) := \sum_{n\geq 1} n a_n x^{n-1}$.

L'opérateur de dérivation est similaire à la notion usuelle de « dérivée » que vous avez apprise en analyse, excepté qu'il est juste défini de manière formelle.

Proposition 4.9. *Soient $f, g \in \mathbb{R}[[x]]$. Alors $\partial(f+g) = \partial(f) + \partial(g)$ et $\partial(fg) = \partial(f)g + f\partial(g)$.*

Démonstration. L'affirmation sur la linéarité est triviale. On montre la formule pour le produit en regardant les termes de la « base » des séries formelles x^n : $\partial(x^n \cdot x^m) = \partial(x^{n+m}) = (n+m)x^{n+m-1}$. D'un autre côté, $\partial(x^n)x^m + \partial(x^m)x^n = (n+m)x^{n+m-1}$. □

Corollaire 4.10. *Soient $f, g, h \in \mathbb{R}[[x]]$ et supposons que $f = g/h$. Alors*

$$\partial(f) = \frac{h\partial(g) - g\partial(h)}{h^2}.$$

Démonstration. On sait que $fh = g$ et par la proposition 4.9 on a $h\partial(f) + f\partial(h) = \partial(g)$, c'est-à-dire $h\partial(f) = \partial(g) - f\partial(h)$. En multipliant les deux côtés par h et en remarquant que $fh = g$, on obtient $h^2\partial(f) = h\partial(g) - g\partial(h)$, ce que l'on voulait montrer. □

Une application immédiate de l'opérateur de dérivation est la suivante.

Proposition 4.11. *On a $\sum_{n\geq 0} nx^n = x/(1-x)^2$.*

Démonstration. On a $\sum_{n\geq 0} nx^n = x\sum_{n\geq 0} nx^{n-1} = x\partial(\sum_{n\geq 0} x^n) = x\partial(1/(1-x))$. D'après la proposition précédente $\partial(1/(1-x)) = 1/(1-x)^2$ et on obtient donc l'affirmation. □

Exemple 4.12. Pour $n \geq 0$ soit la suite a_n donnée par $a_0 = 0$ et $a_n = 2a_{n-1} + n$ pour $n \geq 1$. On aimerait trouver une formule close pour a_n. Encore une fois, on construit la série génératrice. Soit $f := \sum_{n\geq 0} a_n x^n = \sum_{n\geq 1} a_n x^n$. Alors $f = 2\sum_{n\geq 1} a_{n-1}x^n + \sum_{n\geq 1} nx^n = 2xf + \sum_{n\geq 0} nx^n$. Ainsi, en utilisant la proposition précédente, on trouve que

$$f = \frac{x}{(1-x)^2(1-2x)}.$$

L'astuce est de trouver les valeurs A, B, C qui vérifient $f = A/(1-x)^2 + B/(1-x) + C/(1-2x)$ (il s'agit de la décomposition en éléments simples de f que vous avez peut être déjà vue en analyse pour intégrer un quotient de polynômes). On a

$$\begin{aligned}\frac{A}{(1-x)^2} + \frac{B}{1-x} + \frac{C}{1-2x} &= \frac{A(1-2x) + B(1-x)(1-2x) + C(1-x)^2}{(1-x)^2(1-2x)} \\ &= \frac{(A+B+C) + (-2A-3B-2C)x + (2B+C)x^2}{(1-x)^2(1-2x)}.\end{aligned}$$

On doit donc avoir

$$\begin{aligned} A + B + C &= 0 \\ -2A - 3B - 2C &= 1 \\ 2B + C &= 0 \end{aligned}$$

L'unique solution de ce système d'équations est $A = B = -1, C = 2$. Ainsi,

$$f = -\frac{1}{(1-x)^2} - \frac{1}{1-x} + \frac{2}{1-2x}.$$

Remarquez que $1/(1-x)^2 = \partial(1/(1-x)) = \sum_{n\geq 0} nx^{n-1} = \sum_{n\geq 0}(n+1)x^n$, que $1/(1-x) = \sum_{n\geq 0} x^n$, et que $2/(1-2x) = \sum_{n\geq 0} 2^{n+1}x^n$. On en déduit

$$f = \sum_{n\geq 0} \left(-n - 2 + 2^{n+1}\right) x^n.$$

Et donc que $a_n = 2^{n+1} - n - 2$ pour tout $n \geq 0$. ◇

4.1.3. Nombre de partitions d'un ensemble à n éléments

Quel est le nombre de partitions en k parties de $\underline{n}$? En d'autres termes, quel est le nombre de relations d'équivalence que l'on peut définir sur $\underline{n}$ et qui ont exactement k classes d'équivalences ? Ce nombre est noté $\left\{ {n \atop k} \right\}$ et est appelé un *nombre de Stirling de seconde espèce*. On va trouver une formule close pour ces nombres à l'aide des fonctions génératrices.

Commençons par traiter les cas particuliers. Si $k > n$, alors de manière évidente $\left\{ {n \atop k} \right\} = 0$. Si $k = 0$ et $n \neq 0$, alors $\left\{ {n \atop k} \right\} = 0$. On définit $\left\{ {0 \atop 0} \right\} = 1$.

Lemme 4.13. *On a pour tout* $(n, k) \neq (0, 0)$ *et* $0 \leq k \leq n$ *:*

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}.$$

Démonstration. Une partition de $\underline{n}$ en k parties peut avoir l'une des deux formes suivantes : soit la partie qui contient l'élément $n-1$ est formée d'un seul élément, soit elle en a plusieurs. Dans le premier cas, on sépare l'élément $n-1$ des autres et on obtient une partition de $\underline{n-1}$ en $k-1$ parties. Dans le second cas, on obtient une partition de $\underline{n-1}$ en k parties. Réciproquement, si on a une partition de $\underline{n-1}$ en $k-1$ parties, on peut créer de façon unique une partition de $\underline{n}$ en k parties en prenant pour la $k^{\text{ème}}$ partie l'élément $n-1$ tout seul. Et si on a une partition de $\underline{n-1}$ en k parties, on peut placer l'élément $n-1$ dans n'importe laquelle de ces parties pour obtenir une partition de $\underline{n}$ en k parties. Pour ce dernier cas il y a donc k possibilités, d'où le résultat. □

Maintenant, pour $k \geq 0$, définissons

$$P_k := \sum_{n \geq 0} \left\{ {n \atop k} \right\} x^n.$$

Remarquez que $P_0 = 1$ avec cette notation. Ainsi, le lemme précédent nous montre que

$$\begin{aligned}
P_k &= \sum_{n \geq 0} \left\{ {n \atop k} \right\} x^n \\
&= \sum_{n \geq k} \left\{ {n \atop k} \right\} x^n \\
&= \sum_{n \geq k} \left\{ {n-1 \atop k-1} \right\} x^n + k \sum_{n \geq k} \left\{ {n-1 \atop k} \right\} x^n \\
&= x \sum_{n \geq k} \left\{ {n-1 \atop k-1} \right\} x^{n-1} + xk \sum_{n \geq k} \left\{ {n-1 \atop k} \right\} x^{n-1} \\
&= xP_{k-1} + kxP_k.
\end{aligned}$$

De là, on obtient

$$P_k = \frac{x}{1-kx} P_{k-1}, \quad P_0 = 1.$$

Ce qui nous montre (par récurrence) que

$$P_k = \frac{x^k}{(1-x)(1-2x)(1-3x)\cdots(1-kx)}.$$

Le but est maintenant de trouver une décomposition en éléments simples de la fonction de droite. Pour cela, il suffit de trouver $a_1, \ldots, a_k$ tels que

$$\frac{1}{(1-x)(1-2x)(1-3x)\cdots(1-kx)} = \sum_{r=1}^{k} \frac{a_r}{1-rx}.$$

Pour cela, pour tout $r = 1, 2, \ldots, k$, on multiplie les deux côtés par $1-rx$ et on évalue les deux expressions en $x = 1/r$. Ensuite, le terme de droite vaut a_r, alors que le terme de gauche vaut

$$\frac{1}{(1-1/r)(1-2/r)\cdots(1-(r-1)/r)(1-(r+1)/r)\cdots(1-k/r)} = (-1)^{k-r} \frac{r^{k-1}}{(r-1)!(k-r)!}.$$

On voit donc que

$$\begin{aligned} P_k &= \sum_{r=1}^{k}(-1)^{k-r}\frac{r^{k-1}}{(r-1)!(k-r)!}\sum_{n\geq 0} r^n x^{n+k} \\ &= \sum_{n\geq k}\left(\sum_{r=1}^{k}(-1)^{k-r}\frac{r^{k-1}}{(r-1)!(k-r)!}r^{n-k}\right)x^n \\ &= \sum_{n\geq k}\left(\sum_{r=1}^{k}(-1)^{k-r}\frac{r^{n}}{r!(k-r)!}\right)x^n \end{aligned}$$

et donc que

$$\left\{ {n \atop k} \right\} = \sum_{r=1}^{k}(-1)^{k-r}\frac{r^n}{r!(k-r)!}$$

pour $n, k \geq 0$.

4.1.4. Fonctions génératrices caractéristiques

Considérons le problème suivant : étant donné un entier $n \in \mathbb{N}$, trouver le nombre A_n de quadruplets $(a, b, c, d) \in \mathbb{N}^4$ de somme n tels que

- a est divisible par 3,
- b est inférieur à 6,
- c est divisible par 7,
- d est inférieur à 2.

Comme on peut s'en douter, ce problème n'est pas simple. Par exemple, pour $n = 8$, les possibilités sont les suivantes :

a	6	6	6	3	3	3	0	0	0
b	2	1	0	5	4	3	6	1	0
c	0	0	0	0	0	0	0	7	7
d	0	1	2	0	1	2	2	0	1

si bien que $A_8 = 9$. Afin d'étudier de tels problèmes, on introduit la notation suivante :

Définition 4.14. Soit $S \subseteq \mathbb{N}$. On appelle *fonction génératrice caractéristique de* S, et on note C_S, la fonction

$$C_S := \sum_{n\geq 0}\chi_S(n)x^n,$$

où $\chi_S(n) = 1$ si $n \in S$ et $\chi_S(n) = 0$ sinon.

Exemple 4.15. Supposons que S soit l'ensemble des entiers divisibles par un entier d non nul. Alors $C_S = \sum_{n\geq 0} x^{dn} = 1/(1-x^d)$.

On dispose du résultat suivant :

Théorème 4.16. *Soient $S, T \subseteq \mathbb{N}$ et soit $A_n := |\{(a, b) \in S \times T \mid a + b = n\}|$. Alors*

$$\sum_{n\geq 0} A_n x^n = C_S \cdot C_T.$$

Démonstration. On a

$$C_S C_T = \sum_{n\geq 0}\left(\sum_{k=0}^{n}\chi_S(k)\chi_T(n-k)\right)x^n.$$

Notons que $\chi_S(k)\chi_T(n-k) = 1$ ssi $k \in S, n-k \in T$ et $\chi_S(k)\chi_T(n-k) = 0$ sinon. Il s'ensuit que

$$\sum_{k=0}^{n}\chi_S(k)\chi_T(n-k) = |\{(m, n-m) \mid m \in S, n-m \in T\}| = |\{(a, b) \in S \times T \mid a + b = n\}| = A_n,$$

ce qui prouve le théorème. □

En raisonnant par récurrence, le résultat précédent s'étend comme suit :

Théorème 4.17. *Soient $S_1, S_2, \ldots, S_t \subseteq \mathbb{N}$, et pour $n \in \mathbb{N}$ posons*

$$A_n := |\{(a_1, \ldots, a_t) \in S_1 \times \cdots \times S_t \mid a_1 + \cdots + a_t = n\}|.$$

Alors on a

$$\sum_{n\geq 0} A_n x^n = C_{S_1} \cdot C_{S_2} \cdots C_{S_t}.$$

Armés de ce résultat, nous pouvons désormais résoudre le problème de dénombrement du début du paragraphe. À cette fin, soient S_1 l'ensemble des entiers divisibles par 3, S_2 l'ensemble des entiers inférieurs à 6, S_3 l'ensemble des entiers divisibles par 7 et S_4 l'ensemble des entiers inférieurs à 2. On a alors

$$\begin{aligned} C_{S_1} &= \sum_{n\geq 0} x^{3n} = \frac{1}{1-x^3} \\ C_{S_2} &= 1 + x + \cdots + x^6 = \frac{1-x^7}{1-x} \\ C_{S_3} &= \sum_{n\geq 0} x^{7n} = \frac{1}{1-x^7} \\ C_{S_4} &= 1 + x + x^2 = \frac{1-x^3}{1-x}. \end{aligned}$$

Ainsi, grâce au théorème 4.17, si $A_n = |\{(a,b,c,d) \in S_1 \times \cdots \times S_4 \mid a+b+c+d = n\}|$, alors

$$\sum_{n\geq 0} A_n x^n = \prod_{i=1}^{4} C_{S_i} = \frac{1}{1-x^3}\frac{1-x^7}{1-x}\frac{1}{1-x^7}\frac{1-x^3}{1-x} = \frac{1}{(1-x)^2}.$$

Comme $1/(1-x)^2 = \partial(1/(1-x)) = \sum_{n\geq 0}(n+1)x^n$, on en déduit que $A_n = n+1$.

Comme autre exemple, calculons pour tout $n \in \mathbb{N}$ le nombre B_n de triplets $(a,b,c) \in \mathbb{N}^3$ tels que $a+b+c = n$. Dans ce cas, $S_1 = S_2 = S_3 = \mathbb{N}$ et on a

$$\sum_{n\geq 0} B_n x^n = \left(\frac{1}{1-x}\right)^3.$$

Mais $\frac{1}{(1-x)^3} = \partial(1/(1-x)^2)/2$, si bien que

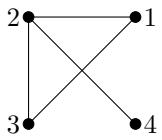
$$\begin{aligned} \sum_{n\geq 0} B_n x^n &= \frac{1}{(1-x)^3} \\ &= \frac{1}{2}\partial\left(\frac{1}{(1-x)^2}\right) \\ &= \frac{1}{2}\sum_{n\geq 1} n(n+1)x^{n-1} \\ &= \frac{1}{2}\sum_{n\geq 0}(n+1)(n+2)x^n \\ &= \sum_{n\geq 0}\binom{n+2}{2}x^n, \end{aligned}$$

et finalement $B_n = \binom{n+2}{2}$.

4.2. Double comptage

Théorème 4.18. *Soit G un graphe avec n sommets qui ne contient pas $K_{2,2}$ comme sous-graphe. Alors G a au plus $(n^{3/2}+n)/2$ arêtes.*

Démonstration. Notons V l'ensemble des sommets de G et E l'ensemble de ses arêtes. Considérons alors la matrice M avec $\binom{n}{2}$ lignes et n colonnes : les lignes de cette matrice sont indexées par les ensembles $\{v, v'\}$ avec $v, v' \in V$; les colonnes sont indexées par les éléments de V. Il y a un 1 à l'intersection d'une ligne $\{v, v'\}$ et d'une colonne u ssi v et v' sont tous deux voisins de u. Voici un exemple de la matrice M pour le graphe ci-dessous :



	1	2	3	4
{1,2}	0	0	1	0
{1,3}	0	1	0	0
{1,4}	0	1	0	0
{2,3}	1	0	0	0
{2,4}	0	0	0	0
{3,4}	0	1	0	0

On va compter le nombre N de 1 dans cette matrice de deux façons différentes : colonne par colonne et ligne par ligne. Dans chaque ligne, on a au plus un 1, sinon il existe deux sommets $v, v' \in V$ et deux sommets $u, u' \in V$ tels que v et v' sont tous deux voisins de u et de u'. C'est une contradiction car le graphe ne contient pas de sous-graphe isomorphe à $K_{2,2}$ par hypothèse. Ainsi, N est majoré par le nombre de lignes de M, c'est-à-dire $N \leq \binom{n}{2}$. Regardons maintenant le nombre de 1 dans une colonne correspondant à $u \in V$. Si u est de degré d, alors cette colonne a $\binom{d}{2}$ 1, un pour chaque paire de sommets auxquels u est relié. Si $d_1, \ldots, d_n$ est la suite des degrés de G, on a donc

$$N = \sum_{i=1}^{n} \binom{d_i}{2} \leq \binom{n}{2},$$

ce qui nous donne

$$\sum_{i=1}^{n} (d_i - 1)^2 < 2 \sum_{i=1}^{n} \binom{d_i}{2} \leq 2\binom{n}{2} < n^2.$$

En appliquant maintenant l'inégalité de Cauchy-Schwarz aux vecteurs $x = (d_1 - 1, \ldots, d_n - 1)$ et $y = (1, 1, \ldots, 1)$ de $\mathbb{R}^n$ on obtient

$$||y \cdot x||^2 = \left(\sum_{i=1}^{n} (d_i - 1) \right)^2 \leq ||y||^2 ||x||^2 = n \sum_{i=1}^{n} (d_i - 1)^2 \leq n^3,$$

c'est-à-dire $\sum_{i=1}^{n} (d_i - 1) \leq n^{3/2}$ et

$$|E| = \frac{1}{2} \sum_{i=1}^{n} d_i \leq \frac{1}{2}(n^{3/2} + n).$$

Cela termine la preuve. □

Pour le théorème suivant, nous avons besoin de la notion de distance de Hamming entre deux vecteurs binaires.

Définition 4.19. La *distance de Hamming* $d_H(x, y)$ entre deux vecteurs binaires $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$ est le nombre de positions où les deux vecteurs diffèrent : $d_H(x, y) = |\{i \mid x_i \neq y_i\}|$.

Théorème 4.20 (Plotkin)**.** *Supposons que l'on ait N vecteurs binaires de dimension n tels que la distance de Hamming entre n'importe quelle paire de vecteurs soit au moins d. Alors, si $d > n/2$, on a $N \leq 2d/(2d - n)$.*

Démonstration. On écrit les N vecteurs dans une matrice A de taille $N \times n$ pour laquelle chaque ligne correspond à l'un de ces vecteurs. Notons S l'ensemble de ces vecteurs. On aimerait calculer le nombre $M := \sum_{x,y \in S, x \neq y} d_H(x, y)$ de deux façons différentes, où $d_H(x, y)$ est la distance de Hamming entre x et y.

Premièrement, comme on sait que $d_H(x, y) \geq d$, on obtient

$$M \geq dN(N - 1),$$

car il y a $N(N-1)$ paires ordonnées d'éléments de S. Ensuite, on regarde les colonnes de la matrice A. Supposons que l'on ait m_i 1 dans la $i^{\text{ème}}$ colonne. Alors la contribution de cette colonne à M est $2m_i(N - m_i)$: c'est le nombre de paires de vecteurs qui diffèrent sur la position i. Ainsi

$$dN(N-1) \leq M = \sum_{i=1}^{n} 2m_i(N - m_i) = \sum_{i=1}^{n} (N^2 - (m_i^2 + (N - m_i)^2)) \leq nN^2 - \frac{1}{2} \sum_{i=1}^{n} (m_i + N - m_i)^2 = \frac{nN^2}{2}.$$

Finalement, $d(N-1) \leq nN/2$, i.e., $N(2d-n) \leq 2d$, ce qui implique notre affirmation. □

4.3. La méthode probabiliste

Dans cette section, nous nous intéressons à démontrer l'existence de certaines structures combinatoires. Pour cela, la méthode probabiliste consiste à définir une variable aléatoire dont l'espérance correspond au nombre moyen de telles structures. En montrant que cette espérance est positive, on peut ainsi montrer l'existence de telles structures. On va montrer quelques exemples de cette méthode.

4.3.1. 2-Coloriage d'ensemble

Définition 4.21. Soient X un ensemble fini et $\mathcal{M} \subseteq P(X)$. $\mathcal{M}$ est dit 2-*coloriable* s'il existe une fonction $f\colon X \to \{0,1\}$ telle que pour tout $S \in \mathcal{M}$ il existe $x, y \in S$ tels que $f(x) \neq f(y)$, c'est à dire que tous les éléments de $\mathcal{M}$ contiennent les deux couleurs.

Supposons que chaque ensemble dans $\mathcal{M}$ a exactement k éléments. Quel est la plus petite taille $m(k)$ de $\mathcal{M}$ pour laquelle $\mathcal{M}$ n'est pas 2-coloriable ? Pour s'échauffer, voici un résultat.

Proposition 4.22. *On a* $m(2) = 3$.

Démonstration. Dans ce cas, les sous-ensembles dans $\mathcal{M}$ peuvent être vus comme des arêtes d'un graphe avec comme sommets X et on veut savoir quand le graphe est biparti. S'il n'est pas biparti, il a au moins 3 arêtes et donc $m(2) \geq 3$. D'un autre côté, si $|X| = 3$ et $\mathcal{M}$ est l'ensemble de tous les sous-ensembles à 2 éléments de X, alors $\mathcal{M}$ n'est pas 2-coloriable. On a donc $m(2) \leq 3$ et donc $m(2) = 3$. □

Il est déjà plus difficile de prouver que $m(3) = 7$; nous ne le ferons pas dans ce cours. Avec la méthode probabiliste, on va montrer le théorème suivant :

Théorème 4.23. *On a* $m(k) \geq 2^{k-1}$*, c'est-à-dire, si* $\mathcal{M}$ *contient moins de* 2^{k-1} *éléments, alors il est* 2*-coloriable.*

Démonstration. La stratégie de la preuve est la suivante : on va colorier les éléments de X aléatoirement. On assigne ainsi à chaque élément de manière aléatoire et indépendante une valeur 0 ou 1, chacune avec probabilité $1/2$. Ensuite, on va calculer une borne supérieure sur la probabilité qu'un ensemble de $\mathcal{M}$ soit monochromatique. Si cette probabilité est plus petite que 1, alors on aura montré que la probabilité qu'aucun des éléments de $\mathcal{M}$ soit monochromatique est positive, c'est-à-dire qu'il existe un 2-coloriage de $\mathcal{M}$.

Soit $m = |\mathcal{M}|$ et pour $i = 1, \ldots, m$ soit A_i l'événement « l'ensemble numéro i est monochromatique ». Alors $\Pr[A_i] = 2 \cdot 2^{-k}$: la probabilité que tous les éléments du $i^{\text{ème}}$ ensemble aient la valeur 0 est 2^{-k}, de même pour la valeur 1. La probabilité qu'il y ait un ensemble de $\mathcal{M}$ monochromatique est donc

$$\Pr[A_1 \cup A_2 \cup \cdots \cup A_m] \leq \sum_{i=1}^{m} \Pr[A_i] = m2^{1-k}.$$

Ainsi, si $m < 2^{k-1}$, cette probabilité est plus petite que 1 et la probabilité de l'événement contraire est strictement positive. On vient de montrer que $\mathcal{M}$ est 2-coloriable. □

4.3.2. Le nombre d'indépendance

Théorème 4.24. *Soit* $G = (V, E)$ *un graphe. Alors*

$$\alpha(G) \geq \sum_{v \in V} \frac{1}{\deg(v) + 1}.$$

Démonstration. Sans perte de généralité on peut supposer que $V = \underline{n}$. Soit π une variable aléatoire sur l'ensemble des permutations de V, avec $\Pr[\pi] = 1/n!$. Soit $M(\pi)$ l'ensemble de tous les sommets $v \in V$ tels que pour tous les voisins w de v on ait $\pi(w) > \pi(v)$. Alors, $M(\pi)$ est un ensemble indépendant : sinon, si $v, w \in M(\pi)$ et $(v, w) \in E$, alors $\pi(v) > \pi(w)$ et $\pi(w) > \pi(v)$, ce qui n'est pas possible. On en déduit pour tout π :

$$\alpha(G) \geq |M(\pi)|.$$

Notez que $M(\pi)$ est une variable aléatoire sur $P(V)$, l'ensemble des parties de V. Pour montrer l'affirmation, il suffit de montrer que $\mathrm{E}[|M(\pi)|]$ est plus grande que la partie droite dans la formule du théorème, avec $\mathrm{E}[|M(\pi)|]$ l'espérance de $M(\pi)$. Cela provient du fait que $\mathrm{E}[|M(\pi)|]$ est la taille moyenne de $M(\pi)$ et que si cette taille moyenne est d'au moins q, alors il existe certains π pour lesquels $M(\pi)$ a au moins q éléments. On a

$$\mathrm{E}[|M(\pi)|] = \sum_{v \in V} \Pr[v \in M(\pi)].$$

Si π est une permutation choisie aléatoirement et uniformément parmi l'ensemble de toutes les permutations de V, alors tous les ordres possibles de l'ensemble $N_v \cup \{v\}$ sont équiprobables, avec N_v l'ensemble des voisins de v. Il s'ensuit que la probabilité que $\pi(v)$ est plus petite que $\pi(w)$ pour tout $w \in N_v$ est $1/(\deg(v)+1)$, donc

$$\mathrm{E}[|M(\pi)|] = \sum_{v \in V} \frac{1}{\deg(v)+1},$$

ce qui prouve le théorème. □

4.3.3. Grand sous-graphe biparti

Théorème 4.25. *Soit $G = (V, E)$ un graphe avec $2n$ sommets et $m > 0$ arêtes. Alors il existe une partition de V en sous-ensembles A et B, chacun de taille n, tel qu'il y a au moins $m/2$ arêtes entre A et B, c'est-à-dire, $|\{(x, y) \in E \mid x \in A \wedge y \in B\}| \geq m/2$.*

Démonstration. On choisit un sous-ensemble A de taille n de V de manière uniforme et aléatoire parmi tous les $\binom{2n}{n}$ choix possibles et l'on pose $B := V - A$. Ainsi, A est une variable aléatoire. Soit N le nombre d'arêtes entre A et B. N est également une variable aléatoire. On va montrer que $\mathrm{E}[N] \geq m/2$, ce qui montre qu'il existe un ensemble A tel que le nombre d'arêtes entre A et B est d'au moins $m/2$.

Pour calculer $\mathrm{E}[N]$, on va, pour toute arête du graphe, calculer la probabilité que cette arête relie un sommet de A à un sommet de B. Plus précisément, pour toute arête e on définit la variable aléatoire X_e sur $\{0, 1\}$ dont la valeur est zéro ssi les deux sommets de e appartiennent tous les deux à A ou à B. Alors $N = \sum_{e \in E} X_e$ et par linéarité de l'espérance, $\mathrm{E}[N] = \sum_{e \in E} E[X_e]$. Remarquez que $\mathrm{E}[X_e] = 1 \Pr[X_e = 1] + 0 \Pr[X_e = 0] = \Pr[X_e = 1]$, donc

$$\mathrm{E}[N] = \sum_{e \in E} \Pr[X_e = 1].$$

On va montrer que $\Pr[X_e = 1] > 1/2$. Pour cela, soient u et v les deux sommets de l'arête e. Si on impose que $u \in A$, mais que $v \notin A$, alors on peut choisir les $n-1$ éléments restants de A de $\binom{2n-2}{n-1}$ façons. On obtient le même nombre de choix pour A si on impose que $u \notin A$ et $v \in A$. Ainsi,

$$\Pr[X_e = 1] = 2\frac{\binom{2n-2}{n-1}}{\binom{2n}{n}} = \frac{n}{2n-1} > \frac{1}{2}.$$

On en déduit que $\mathrm{E}[N] = \sum_{e \in E} \frac{n}{2n-1} > \sum_{e \in E} 1/2 = m/2$, ce qui prouve le théorème. □