MATH-F-307 Mathématiques discrètes

Samuel Fiorini

Version du 18 décembre 2012

Table des matières

Remerciements

Ce syllabus se base en partie sur une retranscription électronique du cours oral effectuée par Jérémy Pagé en 2010–2011, avec l'aide d'Antoine Dewilde, Valérie Pirenne, Yves-Rémi Van Eycke, Sophie Vervier et Jérémy Vion. Je remercie vivement Jérémy et ses camarades de classe pour leur remarquable travail, qui profitera aux générations d'étudiants à venir.

En 2011-2012, Thomas Chapeaux et Joachim Kotek m'ont fait part de diverses erreurs et fautes de frappes. Merci à eux.

Certains des sujets et des énoncés d'exercices dans ce syllabus ont été empruntés au titulaire précédent du cours, Jean Doyen. En tant qu'étudiant, j'ai eu la chance de bénéficier de ses grands talents pédagogiques. Je le remercie vivement.

Last but not least, je remercie Eglantine Camby pour sa relecture attentive de ce syllabus.

Samuel Fiorini.
Bruxelles, le 18 décembre 2012.

Chapitre 1

Comptage élémentaire

1.1 Principes de base

1.1.1 Rappels sur les fonctions

Considérons deux ensembles quelconques A et B.

Définition 1.1. Une fonction f de A vers B est dite *injective* si les images par f de deux éléments distincts de A sont toujours distinctes. De manière équivalente, $f : A \to B$ est injective si et seulement si

$$\forall a, a' \in A : f(a) = f(a') \implies a = a' .$$

Une fonction injective est également appelée *injection*.

Définition 1.2. Une fonction f de A vers B est dite *surjective* si tout élément de B est l'image par f d'au moins un élément de A. En d'autres termes, $f : A \to B$ est surjective si et seulement si

$$\forall b \in B : \exists a \in A : f(a) = b .$$

Cette condition se note également $f(A) = B$. Une fonction surjective est également appelée *surjection*.

Définition 1.3. Une fonction est dite *bijective* si elle est en même temps injective et surjective. On parle alors de *bijection*.

Théorème 1.4. *Soit $f : A \to B$ une fonction. Alors f est une bijection si et seulement si il existe une fonction $g : B \to A$ telle que $g \circ f$ est l'identité sur A et $f \circ g$ est l'identité sur B.*

Démonstration. Pour la partie "seulement si" il suffit de prendre $g = f^{-1}$, l'application réciproque de g.

Pour la partie "si", on vérifie tout d'abord que f est injective. Pour $a, a' \in A$, on voit que $f(a) = f(a')$ implique $g(f(a)) = g(f(a'))$ et donc $a = a'$ car $g \circ f$ est l'identité sur A. On vérifie enfin que f est surjective. Pour $b \in B$, prenons $a := g(b)$. On a alors $f(a) = f(g(b)) = b$ car $f \circ g$ est l'identité sur B. La fonction f étant simultanément injective et surjective, est bien bijective. □

Définition 1.5. L'ensemble des fonctions de A vers B est noté B^A. C'est-à-dire,

$$B^A := \{f : A \to B\} .$$

1.1.2 Cardinalité

Définition 1.6. Pour $n \in \mathbb{N}$, on définit

$$[n] := \{1, \ldots, n\} .$$

Donc $[1] = \{1\}$, $[2] = \{1, 2\}$, etc… De plus, $[0] = \varnothing$.

Définition 1.7. Deux ensembles ont la même *cardinalité*, ou même *taille*, s'il existe une bijection de l'un vers l'autre. Si A et B ont la même cardinalité, on écrit $|A| = |B|$. Un ensemble E est *fini* s'il a la même cardinalité que $[n]$, pour un certain $n \in \mathbb{N}$. On note alors $|E| = n$, ou parfois $\#E = n$.

Théorème 1.8. *Soient A, B deux ensembles* finis, de même cardinalité, *et $f : A \to B$ une fonction. Alors les conditions suivantes sont équivalentes :*

(i) *f est injective ;*

(ii) *f est surjective ;*

(iii) *f est bijective.*

Théorème 1.9 (Principe d'addition)**.** *Si $A_1, \ldots, A_k$ sont des ensembles* finis disjoints, *alors*

$$\left| \bigcup_{i=1}^{k} A_i \right| = |A_1 \cup \cdots \cup A_k| = |A_1| + \cdots + |A_k| = \sum_{i=1}^{k} |A_i| .$$

Définition 1.10. Si $A_1, \ldots, A_k$ sont des ensembles quelconques, alors leur *produit cartésien* est l'ensemble des k-uples $(a_1, \ldots, a_k)$ avec $a_i \in A_i$ pour $i \in [k]$. Il est noté $\prod_{i=1}^{k} A_i$, ou $A_1 \times \cdots \times A_k$. Donc,

$$\prod_{i=1}^{k} A_i = A_1 \times \cdots \times A_k := \{(a_1, \ldots, a_k) \mid \forall i \in [k] : a_i \in A_i\} .$$

Théorème 1.11 (Principe de multiplication)**.** *Si $A_1, \ldots, A_k$ sont des ensembles* finis, *la cardinalité du produit cartésien $A_1 \times \cdots \times A_k$ est le produit des cardinalités des A_i pour $i \in [k]$:*

$$\left| \prod_{i=1}^{k} A_i \right| = |A_1 \times \cdots \times A_k| = |A_1| \cdot \ldots \cdot |A_k| = \prod_{i=1}^{k} |A_i| .$$

Exemple 1.12. Ce n'est pas toujours évident de savoir lequel des deux principes utilisés. C'est bon de se souvenir que ces principes correspondent à des opérations ensemblistes bien distinctes. Dans un cas, c'est la réunion disjointe. Dans l'autre, c'est le produit cartésien.

Prenons par exemple

$$A_1 := \{\text{salade verte, carpaccio}\} \qquad \text{(entrées)} ,$$
$$A_2 := \{\text{spaghetti diable, steak frites, moules}\} \qquad \text{(plats principaux)} .$$

Ici,

$$\#\text{plats} = |A_1 \cup A_2| = 5 \qquad \text{(principe d'addition)},$$
$$\#\text{menus entrée \& plat principal} = |A_1 \times A_2| = |A_1| \cdot |A_2| = 6 \quad \text{(principe de multiplication)}.$$

1.2 Factorielles

Définition 1.13. Pour $n \in \mathbb{N}$, on définit $n!$, la *factorielle* de n, par

$$n! := n \cdot (n-1) \cdot \ldots \cdot 1 .$$

Et quid de 0!, la factorielle de 0 ? Un produit vide est par défaut toujours égal à 1. Donc $0! = 1$. De manière similaire, une somme vide est par défaut toujours égale à 0.

Proposition 1.14. *Pour tout $n \in \mathbb{N}$, $n!$ donne le nombre de bijections d'un ensemble A vers un ensemble B, tous deux de taille n.*

Démonstration. Sans perte de généralité, nous pouvons supposer $A = B = [n]$. Construisons une bijection $f : [n] \to [n]$ en choisissant $f(1)$, puis $f(2)$, puis $f(3)$, etc.... Ayant déterminé $f(1), \ldots, f(i-1)$, nous pouvons choisir $f(i)$ arbitrairement dans l'ensemble $[n] \setminus \{f(1), \ldots, f(i-1)\}$. Cet ensemble ayant $n - i + 1$ eléments, il y a $n - i + 1$ façons de choisir $f(i)$ étant donné $f(1), \ldots, f(i-1)$. Par conséquent, les images de $1, \ldots, n$ par f peuvent être choisies de

$$\prod_{i=1}^{n} (n - i + 1) = n \cdot (n-1) \cdot \ldots \cdot 1$$

façons différentes. □

Par une preuve similaire à la Proposition 1.14, nous obtenons le résultat suivant.

Proposition 1.15. *Pour tout $n \in \mathbb{N}$, le nombre d'injections d'un ensemble A de taille k vers un ensemble B de taille n, est égal à $n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$.*

Notons qu'une injection f de $[k]$ dans $[n]$ peut s'interpréter comme une sélection ordonnée de k objets parmi n, sans répétition. Le i-ème objet sélectionné sera alors donné par $f(i)$.

Le nombre d'*ordres totaux* sur un ensemble à n éléments est $n!$. Par exemple, le nombre d'ordres totaux sur $E = \{a, b, c\}$ est $3! = 3 \cdot 2 \cdot 1 = 6$:

$$\begin{array}{lll} a < b < c & b < a < c & c < a < b \\ a < c < b & b < c < a & c < b < a \end{array}$$

Notons que $n!$ grandit très vite avec n :

n	0	1	2	3	4	5	6	$\cdots$	10	$\cdots$
$n!$	1	1	2	6	24	120	720		3 625 800	

Au-delà de $n = 10$, la factorielle de n devient très rapidement énorme : l'ensemble des ordres totaux sur $[n]$ (comme l'ensemble des bijections de $[n]$ dans $[n]$, etc…) "explose". Même à l'aide d'un ordinateur récent, on aura tout le mal du monde à énumérer tous les ordres totaux sur $[n]$, même pour des valeurs de n relativement petites. On appelle ce phénomène "*explosion combinatoire*". A titre d'exemple, les astronomes estiment que le nombre de particules dans l'univers se situe quelque part entre 54! et 63!. Il serait par conséquent complètement impossible d'énumérer les 64! ordres totaux sur un ensemble de taille 64 et de les stocker dans la mémoire d'un ordinateur. (Sans même parler du temps astronomique que cela prendrait.)

Par un "truc" que Gauss a utilisé pour calculer la somme $1 + 2 + \cdots + n$ (quand il était encore écolier), on peut obtenir une première approximation de $n!$:

$$(n!)^2 = (n \cdot (n-1) \cdot \ldots \cdot 1) \cdot (n \cdot (n-1) \cdot \ldots \cdot 1) = \prod_{k=1}^{n} (n-k+1) \cdot k$$

Remarquons que, pour n fixé, $k \mapsto (n-k+1) \cdot k$ est une fonction quadratique concave dont le maximum est atteint pour $k = (n+1)/2$ et le minimum sur l'intervalle $[1, n]$ est atteint pour $k = 1$ ou $k = n$. Par conséquent, pour $k \in [n]$,

$$n \leqslant (n-k+1) \cdot k \leqslant \left(\frac{n+1}{2}\right)^2$$

et donc (en supposant $n \geqslant 1$)

$$n^n \leqslant (n!)^2 \leqslant 2^{-2n}(n+1)^{2n} \iff n^{n/2} \leqslant n! \leqslant 2^{-n}(n+1)^n \,.$$

En particulier,

$$\frac{1}{2} n \lg n \leqslant \lg n! \leqslant n \lg(n+1) - n \,.$$

1.3 Coefficients binomiaux : définition et premières identités

Définition 1.16. Pour $n, k \in \mathbb{N}$ avec $k \leqslant n$, le *coefficient binomial* $\binom{n}{k}$ (lire "*n choose k*") est égal au nombre de sous-ensembles à k éléments d'un ensemble de n éléments. En particuler, $\binom{n}{0} = \binom{n}{n} = 1$ pour tout $n \in \mathbb{N}$.

Théorème 1.17 (Symétrie). *Pour $n, k \in \mathbb{N}$ avec $k \leqslant n$, on a*

$$\binom{n}{k} = \binom{n}{n-k} \,.$$

Démonstration. Le membre de gauche est la cardinalité de l'ensemble

$$A := \{S \mid S \subseteq [n], |S| = k\}$$

et le membre de droite la cardinalité de l'ensemble

$$B := \{T \mid T \subseteq [n], |T| = n - k\} \,.$$

Considérons la fonction $f : S \mapsto [n] \setminus S$ de A vers B, et la fonction $g : T \mapsto [n] \setminus T$ de B vers A. Etant donné que $g \circ f$ est l'identité sur A et $f \circ g$ est l'identité sur B, il s'en suit que f est une bijection de A vers B (et que $g = f^{-1}$). Les deux ensembles A et B ont donc la même cardinalité. □

Théorème 1.18 (Absorption/extraction). *Pour $n, k \in \mathbb{N}_0$ avec $k \leqslant n$, on a*

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$$

Démonstration. Montrons que

$$\binom{n}{k} k = n\binom{n-1}{k-1}.$$

En vertu du principe de multiplication (voyez-vous pourquoi ?), le membre de droite est la cardinalité de $A := \{(S, e) \mid S \subseteq [n], |S| = k, e \in S\}$ et le membre de droite la cardinalité de $B := \{(e, T) \mid e \in [n], T \subseteq [n] \setminus \{e\}, |T| = k-1\}$. La bijection $(S, e) \mapsto (e, S \setminus \{e\})$ montre que ces deux ensembles ont la même cardinalité. □

Un corollaire de la formule d'absorption/extraction est le développement suivant du coefficient binomial $\binom{n}{k}$:

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{n(n-1)}{k(k-1)}\binom{n-2}{k-2} = \cdots = \frac{n(n-1)\cdots(n-k+1)}{k(k-1)\cdots 1} = \frac{n!}{k!(n-k)!}.$$

Théorème 1.19 (Addition/induction). *Pour $n, k \in \mathbb{N}$ avec $n > k > 0$, on a*

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Démonstration. Fixons un élément $e \in [n]$. Il y a deux types de sous-ensembles $S \subseteq [n]$ de taille k : ceux qui contiennent e, et ceux qui ne contiennent pas e. Cela donne une partition de l'ensemble des sous-ensembles de $[n]$ de taille k en deux ensembles disjoints :

$$\{S \mid S \subseteq [n], |S| = k\} = \{S \mid S \subseteq [n], |S| = k, e \in S\} \cup \{S \mid S \subseteq [n], |S| = k, e \notin S\}.$$

Le premier de ces deux ensembles a $\binom{n-1}{k-1}$ éléments, et le second a $\binom{n-1}{k}$ éléments. On conclut en appliquant le principe d'addition. □

Théorème 1.20 (Somme parallèle). *Pour $m \in \mathbb{N}$ avec $m \geqslant k$:*

$$\sum_{n=k}^{m} \binom{n}{k} = \binom{m+1}{k+1}.$$

Démonstration. On le montre par induction sur m. Pour le cas de base, $m = k$ et donc

$$\sum_{n=k}^{m} \binom{n}{k} = \binom{k}{k} = 1 = \binom{k+1}{k+1} = \binom{m+1}{k+1}.$$

Supposons maintenant que $m > k$ et que la formule est vraie pour les valeurs de m plus petites, et prouvons-là pour un m donné :

$$\sum_{n=k}^{m} \binom{n}{k} = \binom{m}{k} + \sum_{n=k}^{m-1} \binom{n}{k} = \binom{m}{k} + \binom{m}{k+1} = \binom{m+1}{k+1},$$

par la formule d'addition/induction. □

1.4 Coefficients binomiaux : formule du binôme, Δ de Pascal

Pour $x, y \in \mathbb{R}$, on a

$$\begin{array}{rcc} (x+y)^0 & = & 1 \\ (x+y)^1 & = & x+y \\ (x+y)^2 & = & x^2+2xy+y^2 \\ (x+y)^3 & = & x^3+3x^2y+3xy^2+y^3 \\ \vdots & & \vdots \end{array}$$

ou encore

$$\begin{array}{rcc} (x+y)^0 & = & 1x^0y^0 \\ (x+y)^1 & = & 1x^1y^0+1x^1y^0 \\ (x+y)^2 & = & 1x^2y^0+2x^1y^1+1x^0y^2 \\ (x+y)^3 & = & 1x^3y^0+3x^2y^1+3x^1y^2+1x^0y^3 \\ \vdots & & \vdots \end{array}$$

Théorème 1.21 (Formule du binôme de Newton)**.** *Pour tout $n \in \mathbb{N}$,*

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

Démonstration. Distribuons le produit

$$(x+y)^n = \underbrace{(x+y)\cdot\ldots\cdot(x+y)}_{n \text{ fois}} .$$

Chaque terme de l'expression résultante s'obtient en choisissant pour chacune des n parenthèses le terme de gauche (c.-à-d. x) ou le terme de droite (c.-à-d. y). Chacun des termes du produit distribué correspond donc univoquement à un sous-ensemble $S \subseteq [n]$, à savoir l'ensemble des positions des parenthèses où le terme de droite (c.-à-d. y) a été choisi pour former le produit. Donc nous aurons $i \in S$ ssi c'est y qui a été choisi dans la i-ème parenthèse. Le terme correspondant à un sous-ensemble S de taille k est $x^{n-k}y^k$. Ce monôme est obtenu exactement $\binom{n}{k}$ fois dans l'expression. Ceci montre le théorème. □

En s'inspirant de ce qui précède, il est naturel de disposer les coefficients binomiaux en

un triangle infini, le *triangle de Pascal* :

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \\ 1 & & 5 & & 10 & & 10 & & 5 & & 1 \\ & & & & & \vdots & & & & & \end{array}$$

Les triangle obtenu est riche en propriétés. En particulier,

- les coefficients situés sur ses deux côtés sont tous égaux à 1 ;
- chaque coefficient est la somme des deux coefficients situés juste au-dessus (formule d'addition/induction) ;
- le triangle possède un axe de symétrie vertical passant par son milieu (symétrie).

Le triangle de Pascal possède des *lignes* constituées des coefficients binomiaux $\binom{n}{k}$ avec n constant et des *diagonales* (montantes) constituées des coefficients binomiaux $\binom{n}{k}$ avec k constant. (Pour ceux qui se demandent comment obtenir les diagonales descendantes, elles sont obtenues en gardant $n-k$ constant. Nous ne les considérerons plus dans la suite.) La formule de somme parallèle nous permet de calculer la somme des $m-k+1$ premiers coefficients d'une diagonale du triangle de Pascal : la somme est le coefficient juste à droite du coefficient suivant dans la diagonale considérée.

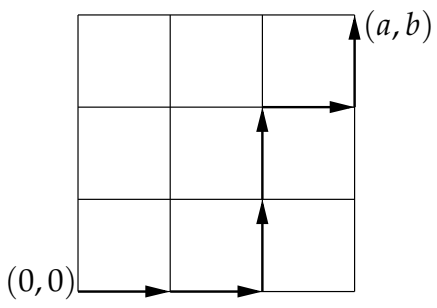
On peut étendre le triangle de Pascal à tout un demi-plan en posant (et c'est naturel vu notre définition) :

$$\binom{n}{k} := 0 \quad \text{quand} \quad k < 0 \text{ ou } k > n \,,$$

pour $n \in \mathbb{N}$. Ceci permet de démontrer les formules obtenues précédemment sans devoir discuter de la position de k par rapport à n. Remarquons qu'il est aussi possible d'étendre le triangle de Pascal au plan tout entier (donc pour les valeurs négatives de n). Mais ceci sort de notre propos.

1.5 Coefficients binomiaux : applications

1. Le nombre de mots de n bits contenant k uns (et donc $n-k$ zéros) est $\binom{n}{k}$ car il y a $\binom{n}{k}$ manières de choisir l'emplacement des k uns. Notez qu'on trouve la même réponse en plaçant les $n-k$ zéros car $\binom{n}{n-k} = \binom{n}{k}$ par symétrie.
2. Le nombre de plus courts chemins de $(0,0)$ à (a,b) dans la grille entière est $\binom{a+b}{a} = \binom{a+b}{b}$ car on peut encoder chaque chemin par un mot de $a+b$ bits avec a uns et b zéros. Par exemple, on peut utiliser la convention suivante : un 1 signifie "se déplacer d'une unité à droite" et un 0 signifie "se déplacer d'une unité vers le haut".



$\longleftrightarrow 110010$

3. Le nombre de solutions $(x_1, \ldots, x_d)$ naturelles (c.-à-d. $(x_1, \ldots, x_d) \in \mathbb{N}^d$) de l'équation $x_1 + x_2 + \cdots + x_d = s$ avec $s \in \mathbb{N}$ est $\binom{s+d-1}{d-1} = \binom{s+d-1}{s}$.
   Par exemple, combien de quadruples de nombres naturels ont une somme de 7 ? On cherche donc à résoudre $x_1 + x_2 + x_3 + x_4 = 7$. Attention, l'ordre est important ! Les vecteurs $(1, 0, 0, 6)$ et $(6, 0, 0, 1)$ sont solutions car $1 + 0 + 0 + 6 = 7 = 6 + 0 + 0 + 1$, mais ces solutions sont différentes.
   L'idée pour obtenir le nombre de solutions est d'encoder une telle solution par un mot sur l'alphabet $\{\circ, |\}$, ou encore par un mot binaire (en remplaçant $\circ$ par 0 et $|$ par 1). Par exemple, $(4, 2, 0, 1)$ est encodé par $\circ\circ\circ\circ|\circ\circ||\circ$ ou 0000100110 en binaire. Ici, les symboles $|$ indiquent les séparations entre les variables x_1, x_2, …, x_d et les $\circ$ indiquent les valeurs des variables. Le nombre de $\circ$ consécutifs donne la valeur de la variable correspondante.
   Donc les mots auxquels on s'intéressent sont tous les mots sur $\{\circ, |\}$ comportant un nombre total de $\circ$ égal à s et un nombre total de $|$ égal à $d - 1$. Il y a $\binom{s+d-1}{d-1} = \binom{s+d-1}{s}$ tels mots.
4. Le nombre de manières de sélectionner k objets pris parmi n, sans ordre, et avec répétition est $\binom{k+n-1}{n-1} = \binom{k+n-1}{k}$. En effet, ce nombre est précisément le nombre de solutions en nombres naturels de $x_1 + x_2 + \cdots + x_n = k$. Par exemple, le nombre de manières d'acheter 20 fruits à un supermarché où il y a 11 sortes de fruits différents est $\binom{20+11-1}{11-1} = \binom{30}{10}$.
   En reprenant les cas vus jusqu'à présent, et y en rajoutant le cas "ordonné" et "avec répétition", on obtient la règle "de quatre" ci-dessous pour le nombre de manières de choisir k objets parmi n.

sélection de k objets pris parmi n	ordonnée	non-ordonnée
sans répétition	$\frac{n!}{(n-k)!} = k!\binom{n}{k}$	$\binom{n}{k}$
avec répétition	n^k	$\binom{n+k-1}{k}$

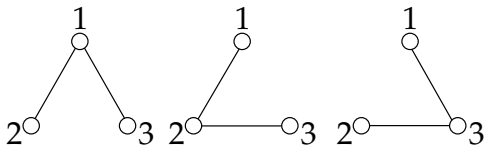
   Notez que le nombre de manière de sélectionner k objets pris parmi n, avec ordre et avec répétition est bien n^k car ce nombre compte le nombre d'éléments de l'ensemble $\underbrace{[n] \times [n] \times \cdots \times [n]}_{k \text{ facteurs}}$ des k-uples de nombres pris dans $[n]$.

1.6 Preuves bijectives

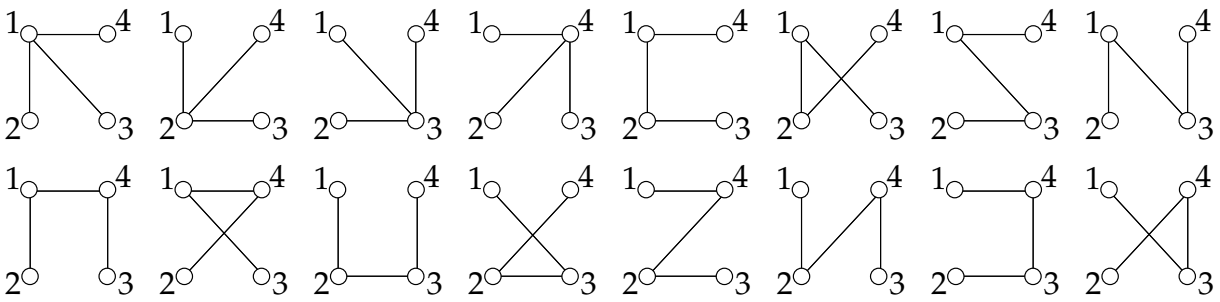
Parfois on peut compter le nombre d'éléments d'un ensemble A en trouvant une bijection entre A et un autre ensemble B dont on connaît le nombre d'éléments. Alors évidemment, $|A| = |B|$.

Théorème 1.22 (Théorème de Cayley, 1889)**.** *Le nombre d'arbres étiquetés à n sommets est exactement n^{n-2}.*

Par exemple, pour $n = 3$, on trouve les $3 = 3^{3-2}$ arbres suivants.



Pour $n = 4$, on trouve les $16 = 4^{4-2}$ arbres suivants.



Démonstration (du théorème de Cayley). Soit a_n le nombre d'arbres étiquetés à n sommets numérotés de 1 à n, et soit $\mathcal{A}_n$ l'ensemble des arbres étiquetés à n sommets numérotés de 1 à n, avec deux sommets spéciaux ◯ et □ (◯ et □ peuvent coincider). ◯ est appelé *extrémité "gauche"* et □ est appelé *extrémité "droite"*.

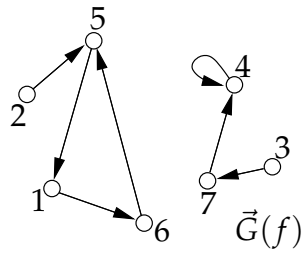
Remarquons qu'on a

$$|\mathcal{A}_n| = n^2 a_n$$

car pour tout arbre à n sommets il y a n choix pour ◯ et n choix pour □. Notre but est de démontrer $|\mathcal{A}_n| = n^n$ en donnant une bijection entre $\mathcal{A}_n$ et $[n]^{[n]}$, l'ensemble des fonctions de $[n]$ dans $[n]$.

Soit $f : [n] \to [n]$ une fonction et soit $\vec{G}(f)$ le graphe dirigé dont les sommets sont les nombres $1, \ldots, n$ et les arcs sont les couples $(i, f(i))$ avec $i \in [n]$ (chaque sommet est lié par un arc vers son image).

Par exemple, pour $n = 7$ et $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 4 & 1 & 5 & 4 \end{pmatrix}$ on a le graphe suivant.



Ici, la fonction f est écrite comme une matrice $2 \times n$. Chaque colonne donne en deuxième ligne l'image de l'élément en première ligne.

Le graphe $\vec{G}(f)$ possède exactement n arcs. De chaque sommet sort exactement un arc (voyez-vous pourquoi ?). Le nombre d'arcs entrant en un sommet varie de 0 à n. On peut voir que chaque composante connexe de $\vec{G}(f)$ contient un unique cycle dirigé.

On définit $\mathcal{M}$ comme l'ensemble des sommets du graphe $\vec{G}(f)$ qui apparaissent sur un cycle dirigé (il peut y avoir plusieurs tels cycles dirigés). Intuitivement, ce sont ces cycles dirigés qui empêchent $\vec{G}(f)$ de définir un arbre. De manière équivalente, on pourrait définir $\mathcal{M}$ comme le plus grand sous-ensemble de $[n]$ sur lequel f est bijective.

Posons $\mathcal{M} := \{i_1, i_2, \ldots, i_m\}$ avec $i_1 < i_2 < \cdots < i_m$ et écrivons la restriction de f à $\mathcal{M}$ comme

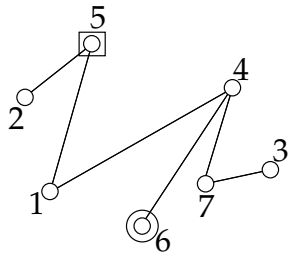
$$f|_{\mathcal{M}} = \begin{pmatrix} i_1 & i_2 & \cdots & i_m \\ f(i_1) & f(i_2) & \cdots & f(i_m) \end{pmatrix}.$$

Pour rappel, la seconde ligne de cette représentation de $f|_{\mathcal{M}}$ (la restriction de f à $\mathcal{M}$) donne le vecteur des images de i_1, i_2, …, i_m. Par définition, $f|_{\mathcal{M}}$ est un bijection de $\mathcal{M}$ vers $\mathcal{M}$, donc tous les éléments de $\mathcal{M}$ apparaissent dans la seconde ligne, dans un certain ordre.

L'idée maintenant est de représenter ce vecteur des images par un chemin dont les sommets sont ◯ $= f(i_1), f(i_2), \ldots, f(i_m) =$ □ (et ainsi se débarasser des cycles). Pour le reste

on utilise les arcs de $\vec{G}(f)$ dont on enlève l'orientation (pour obtenir des arêtes, qui par définition n'ont pas de direction). On obtient ainsi un arbre étiqueté à n sommets dont deux sont distingués, c'est-à-dire un élément de $\mathcal{A}_n$.

Pour l'exemple précédent, avec $n = 7$ et $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 5 & 7 & 4 & 1 & 5 & 4 \end{pmatrix}$, on a $\mathcal{M} = \{1, 4, 5, 6\}$ et $f|_{\mathcal{M}} = \begin{pmatrix} 1 & 4 & 5 & 6 \\ 6 & 4 & 1 & 5 \end{pmatrix}$. Donc $\bigcirc = 6$ (l'extrémité "gauche") et $\square = 5$ (l'extrémité "droite"). Il faut remplacer les cycles dirigés 1–6–5–1 et 4–4 par le chemin 6–4–1–5. L'arbre obtenu est représenté ci-dessous.

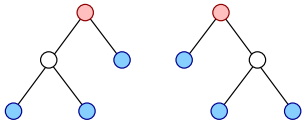


Ceci définit une correspondance (c'est-à-dire une fonction) de $[n]^{[n]}$ vers $\mathcal{A}_n$. A chaque fonction f on fait correspondre exactement un élément de $\mathcal{A}_n$. Cette correspondance est bijective car il existe une correspondance réciproque associant à tout élément de $\mathcal{A}_n$ une fonction f, telle qu'effectuer les deux correspondances l'une après l'autre donne toujours l'identité. La correspondance de départ est une bijection de $[n]^{[n]}$ vers $\mathcal{A}_n$. □

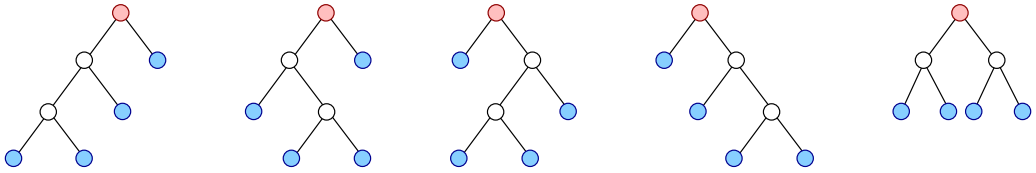
Voyons maintenant un autre exemple de preuve bijective, à propos d'arbres binaires enracinés et triangulations d'un polygone. On l'utilisera dans la suite pour obtenir une formule pour le nombre de triangulations d'un polygone à $n + 1$ côtés, à partir d'une formule pour le nombre d'arbres binaires enracinés à n feuilles. Bien que ces formules ne seront établies que plus tard, le Théorème 1.24 implique que dès qu'on sait compter une sorte d'objets, on sait automatiquement compter l'autre, vu que ensembles correspondants sont en bijection.

Mais qu'appelle-t-on exactement un arbre binaire enraciné à n feuilles ? Par exemple, il y a 1 arbre binaire enraciné à $n = 2$ feuilles.

Il y a 2 arbres binaires enracinés à $n = 3$ feuilles.



Pour $n = 4$ feuilles, il y en a 5.



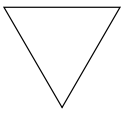
Attention, quand on compte des objets, il faut être bien précis sur ce qu'on compte réellement ! En particulier, sur la manière de décider quand deux objets sont considérés comme égaux, et quand deux objets sont considérés comme différents. Commençons par une définition formelle de ce qu'est un arbre enraciné.

Définition 1.23 (Arbre binaire enraciné)**.** Un *arbre binaire enraciné* est un arbre (c'est-à-dire un graphe connexe, sans cycle) dont tous les sommets ont pour degré 1, 2 ou 3. Un et un seul sommet a pour degré 2, la *racine*. Les sommets de degré 1 sont appelés *feuilles*. Les autres sommets sont les *sommets internes* de l'arbre. Chaque arête porte un label "G" ou "D" (pour "gauche" et "droite").

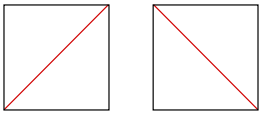
On considère deux arbres binaires comme égaux si l'on peut les superposer l'un sur l'autre sans se préoccuper du nom des sommets, mais en se préoccupant des labels. Ceci n'est évidemment pas une définition formelle. Pour éviter un long détour, disons simplement qu'il suffit de définir la notion d'*isomorphisme* d'arbres binaires enracinés pour obtenir une définition formelle (un exercice pour les plus matheux d'entre vous).

Le problème qui nous intéresse est de compter les arbres binaires enracinés à n feuilles, à isomorphisme près, pour un n donné. Nous ne pouvons pas encore résoudre ce problème (ce sera fait plus tard, au chapitre 3). Par contre, nous pouvons d'ores et déjà faire une observation intéressante : comptons le nombre de triangulations d'un polygone à $n+1$ côtés.

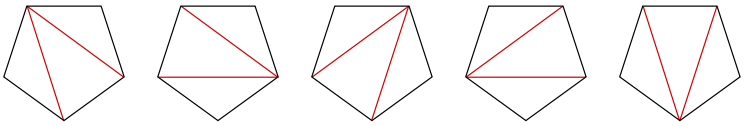
Pour $n = 2$, on trouve 1 triangulation.



Pour $n = 3$, on en trouve 2.



Pour $n = 4$, on en trouve 5.



Aha ! Ces nombres coïncident précisément avec le nombre d'arbres enracinés à n feuilles (comptés à isomorphisme près) pour $n = 2, 3, 4$. Ceci n'est pas un hasard, mais le signe d'un phénomène plus général.

Théorème 1.24. *Le nombre d'arbres binaires enracinés à n feuilles (à isomorphisme près) est égal au nombre de triangulations d'un polygone à $n+1$ côtés.*

Avant de donner une idée de la preuve, voyons ce que signifie ce théorème. On ne sait pas (encore) comment compter les arbres enracinés à n feuilles (à isomorphisme près), ni les triangulations d'un polygone à $n+1$ côtés. Par contre, ce que le Théorème 1.24 montre, c'est que les nombres correspondants sont égaux, et ce pour toute valeur de n ! Dès qu'on pourra compter les objets d'un type, on pourra automatiquement compter les objets de l'autre type.

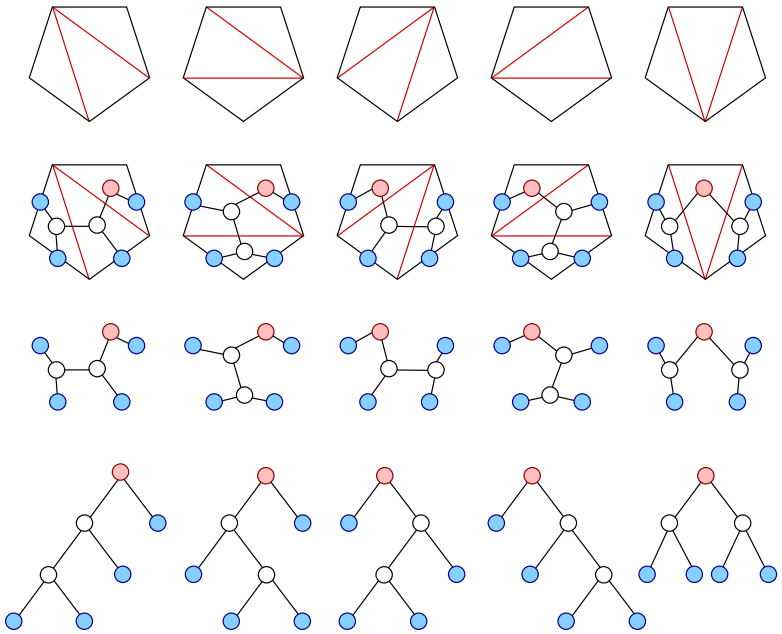
Idée de démonstration (du théorème 1.24). Nous allons fournir une bijection entre l'ensemble $\mathcal{A}_n$ des arbres binaires enracinés à n feuilles, pris à un isomorphisme près, et l'ensemble $\mathcal{T}_{n+1}$ des triangulations d'un $(n+1)$-gone.

Numérotons les côtés d'un $(n+1)$-gone, disons P, de c_0 à c_n dans le sens anti-horlogique (dans la figure ci-dessous, le coté c_0 est représentée en haut).

Etant donné une triangulation de P, nous obtenons un arbre binaire enraciné à n feuilles en plaçant

– la racine dans l'intérieur du triangle adjacent du côté c_0,
– un sommet (interne) dans l'intérieur de chaque autre triangle,
– les n feuilles dans l'intérieur (relatif) des côtés correspondants, de c_1 jusque c_n,

puis en reliant les paires de sommets placés dans des triangles adjacents, ainsi que chaque feuille avec le sommet placé dans le triangle contenant le côté correspondant. Et pour les labels ? On utilise l'orientation du plan. Ces règles définissent une application f de $\mathcal{T}_{n+1}$ dans $\mathcal{A}_n$, qui est illustrée ci-dessous (un dessin vaut parfois mieux qu'un long discours).



Pour compléter la démonstration on démontre que cette application f admet une application g de $\mathcal{A}_n$ dans $\mathcal{T}_{n+1}$ telle que $f \circ g$ et $g \circ f$ sont l'identité sur leurs domaines respectifs. Par le Théorème 1.4, f est une bijection. □

1.7 Coefficients multinomiaux : définition et formule du multinôme

Définition 1.25. Pour $n \in \mathbb{N}$ et $k_1, \ldots, k_t \in \mathbb{N}$ tels que $k_1 + \cdots + k_t = n$, le *coefficient multinomial* $\binom{n}{k_1,\ldots,k_t}$ est le nombre de partitions *ordonnées* d'un ensemble de taille n en t sous ensembles $S_1, \ldots, S_t$ de tailles respectives $k_1, \ldots, k_t$.

Le coefficient multinomial $\binom{n}{k_1,\ldots,k_t}$ peut s'interpréter d'autres manières.

1. C'est le nombre de façons de répartir n objets (distinguables) dans t boîtes (distinguables) de telle sorte à placer k_i objets dans la $i$ème boîte ($i \in [t]$). En d'autres termes, c'est le nombre de fonctions $f : [n] \to [t]$ telles que $|f^{-1}(i)| = k_i$ pour $i \in [t]$.
2. C'est aussi le nombre de mots de n symboles pris dans un alphabet de taille t tels que le nombre d'occurences du $i$ème symbole est k_i ($i \in [t]$).

Exemple 1.26. – Pour tout $n \in \mathbb{N}$, on a $\binom{n}{1,\ldots,1} = n!$ (voyez-vous pourquoi ?).

– Le nombre de mots différents obtenus en permutant les lettres de MASSACHUSETTS est $\binom{13}{2,1,1,1,1,4,2,1}$.
– Le coefficient multinomial $\binom{n}{k,n-k}$ n'est autre que le coefficient binomial $\binom{n}{k}$.

Une propriété importante du coefficient multinomial est qu'on peut permuter librement ses paramètres $k_1, \ldots, k_t$ sans changer sa valeur. (Ceci revient, dans notre seconde interprétation, à permuter les boîtes entre elles.) Donc :

$$\binom{n}{k_1, \ldots, k_t} = \binom{n}{k_{\pi(1)}, \ldots, k_{\pi(t)}}$$

pour toute permutation π de $[t]$. Cette identité généralise l'identité de symétrie des coefficients binomiaux. On peut également généraliser l'identité d'absorption/extraction : dès que $k_1 > 0$, on a

$$\binom{n}{k_1, k_2, \ldots, k_t} = \frac{n}{k_1}\binom{n-1}{k_1 - 1, k_2, \ldots, k_t}.$$

Par symétrie, on a des identités similaires avec $k_2, \ldots, k_t$. Ceci donne un moyen de calculer tout coefficient multinomial en l'exprimant en fonction des factorielles de ses paramètres n, $k_1, \ldots, k_t$. Notons au passage que

$$\binom{n}{0, k_2, \ldots, k_t} = \binom{n}{k_2, \ldots, k_t}.$$

(Si une boîte est vide, on peut l'ignorer.) La formule obtenue est la suivante :

$$\binom{n}{k_1, k_2, \ldots, k_t} = \frac{n!}{k_1!\, k_2! \cdots k_t!}.$$

Et l'identité d'addition/induction ? Elle se généralise également ! En effet, appellons e un des n éléments à répartir dans les t boîtes. Cet élément aboutira fatalement dans une et une seule des t boîtes. Donc, dès que $k_i > 0$ pour tout $i \in [t]$,

$$\binom{n}{k_1, k_2, \ldots, k_t} = \binom{n-1}{k_1 - 1, k_2, \ldots, k_t} + \cdots + \binom{n-1}{k_1, k_2, \ldots, k_t - 1}.$$

Le nom "coefficient multinomial" trouve son origine dans le théorème suivant.

Théorème 1.27 (Formule du multinôme). *Pour tout $n \in \mathbb{N}$ (et tout $x_1, \ldots, x_t \in \mathbb{R}$),*

$$(x_1 + \cdots + x_t)^n = \sum_{k_1 + \cdots + k_t = n} \binom{n}{k_1, \ldots, k_t} x_1^{k_1} \cdots x_t^{k_t},$$

où la somme est effectuée sur tous les tuples $(k_1, \ldots, k_t) \in \mathbb{N}^t$ sommant à n.

1.8 Coefficients multinomiaux : application

Tout arbre (fini) $T = (V, E)$ possède une feuille, c'est-à-dire un sommet de degré 1 (à condition que T ait au moins deux sommets). Si on retire cette feuille, on trouve un nouvel arbre T' avec un sommet de moins. Si n désigne le nombre de sommets de l'arbre T de

départ, alors T' a $n-1$ sommets. En continuant d'effeuiller ainsi notre arbre, on aboutira nécessairement à un arbre ayant un seul sommet. Chaque fois qu'une feuille de l'arbre courant est retirée, une et une seule arête disparaît de l'arbre. Le nombre d'arêtes de T est donc exactement $n-1$, le nombre de sommets retirés avant de terminer avec un seul sommet. Donc

$$|E| = n - 1 \,.$$

Remarque 1.28 (Code de Prüfer)**.** Le processus d'effeuillage décrit ci-dessus donne lieu au *code de Prüfer* d'un arbre, un vecteur à $n-2$ composantes dont la $i$ème composante est l'étiquette du *voisin* du $i$ème sommet enlevé dans l'arbre courant. Deux précisions : premièrement, à chaque étape on choisit toujours la feuille qui a la plus petite étiquette ; deuxièmement, on arête d'écrire le code dès qu'il ne reste plus que deux sommets. Pour fixer les idées, prenons $V = [n]$. Alors le code de Prüfer de l'arbre T est $(n-2)$-uple dont chaque composante est dans $[n]$. On peut vérifier que tout arbre sur $[n]$ peut être reconstruit à partir de son code de Prüfer, et que tout $(n-2)$-uple dont chaque composante est dans $[n]$ est le code de Prüfer d'un arbre sur $[n]$. (Voir exercices.)

Dans tout graphe, la somme des degrés est exactement deux fois le nombre d'arêtes (car chaque arête a deux extrémités). Donc en particulier pour notre arbre $T = (V, E)$,

$$\sum_{v \in V} d(v) = 2|E| \,.$$

Etant donné que T est un arbre, $|E| = n - 1$ et on trouve

$$\sum_{v \in V} d(v) = 2n - 2 \,.$$

La somme des degrés des sommets d'un arbre est deux fois son nombre de sommets, moins deux. Autrement dit, le vecteur des degrés d'un arbre à n sommets est un vecteur de n entiers strictement positifs dont la somme vaut $2n-2$. De manière surprenante, ceci est une caractérisation des vecteurs des degrés des arbres !

Lemme 1.29. *Un vecteur d'entiers strictement positifs $(d_1, \ldots, d_n)$ est le vecteur des degrés d'un arbre à $n \geqslant 2$ sommets (c'est-à-dire il existe un arbre à n sommets dont le $i$ème sommet a pour degré d_i) si et seulement si*

$$\sum_{i=1}^{n} d_i = 2n - 2 \,.$$

Démonstration. Comme le "si" a déjà été prouvé plus haut, montrons le "seulement si", par induction sur n. Le résultat étant clairement vrai pour $n = 2$, supposons que $n \geqslant 3$ et que le résultat est vrai pour moins de n sommets.

Par hypothèse, tous les d_i sont au moins 1 (étant des entiers strictement positifs). Mais ils ne peuvent pas être tous égaux à 1 car sinon $\sum d_i \leqslant n < 2n - 2$. Donc un des d_i est au moins 2. Mais on ne peut avoir $d_i \geqslant 2$ pour tout i car sinon $\sum d_i \geqslant 2n > 2n - 2$. Donc il existe un indice j tel que $d_i \geqslant 2$ et un indice k tel que $d_k = 1$. On peut supposer que $k = n$. Par l'hypothèse d'induction,

$$(d_1, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_{n-1})$$

est le vecteur des degrés d'un arbre à $n-1$ sommets, car sa somme est$2n-4 = 2(n-1)-2$. Donc il existe un arbre T' ayant $n-1$ sommets et $(d_1, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots, d_{n-1})$ comme vecteur de degrés. Rajoutons un $n$ème sommet à cet arbre, ainsi qu'une arête entre le $j$ème sommet et le $n$ème sommet. On obtient un arbre T ayant $(d_1, \ldots, d_{j-1}, (d_j - 1) + 1, d_{j+1}, \ldots, d_{n-1}, 1) = (d_1, \ldots, d_n)$ comme vecteur de degrés. Ce vecteur est donc bien le vecteur des degrés d'un arbre à n sommets. □

Maintenant que nous comprenons très bien les vecteurs des degrés des arbres à n sommets, voyons comment compter le nombre d'arbres ayant un vecteur de degrés donné.

Théorème 1.30. *Soit $(d_1, \ldots, d_n)$ un vecteur de $n \geqslant 2$ entiers strictement positifs sommant à $2n-2$. Le nombre d'arbres à n sommets ayant $(d_1, \ldots, d_n)$ comme vecteur de degrés est*

$$\binom{n-2}{d_1 - 1, \ldots, d_n - 1}.$$

Démonstration. Dans notre preuve du Théorème 1.22, nous avons défini une bijection associant à toute fonction de $[n]$ dans $[n]$ un arbre étiqueté à n sommets dont deux sont spéciaux : ◯ ("extrémité gauche") et □ ("extrémité droite"). Nous allons réutiliser cette bijection pour montrer le résultat.

Etant donné que $\sum d_j = 2n-2$ et que les d_i sont des entiers strictement positifs, $d_j = 1$ pour au moins *deux* indices j. (Ceci traduit le fait que tout arbre possède au moins deux feuilles.) Supposons, sans perte de généralité, que $d_1 = d_n = 1$. Maintenant, considérons toutes les fonctions $f : [n] \to [n]$ telles que

(i) $f(1) = 1$ et $f(n) = n$;

(ii) pour $2 \leqslant j \leqslant n-1$, le nombre d'indices i tels que $f(i) = j$ est exactement $d_j - 1$ (de manière plus concise, $|f^{-1}(j)| = d_j - 1$).

Le nombre de telles fonctions f est le coefficient multinomial

$$\binom{n-2}{d_2 - 1, \ldots, d_{n-1} - 1} = \binom{n-2}{0, d_2 - 1, \ldots, d_{n-1} - 1, 0} = \binom{n-2}{d_1 - 1, \ldots, d_n - 1}.$$

Pour chacune de ces fonctions f, l'ensemble $\mathcal{M} = \{i_1, \ldots, i_m\}$ des sommets du graphe dirigé $\vec{G}(f)$ apparaissant sur un cycle dirigé contient toujours 1 (comme élément minimum : $i_1 = 1$) et n (comme élément maximum : $i_m = n$), car $f(1) = 1$ et $f(n) = n$. Il résulte qu'on a toujours ◯ $= 1$ et □ $= n$.

On peut vérifier que l'arbre correspondant à toute fonction f satisfaisant (i) et (ii) a $(d_1, \ldots, d_n)$ comme vecteur de degrés. En outre, on peut vérifier qu'en inversant la correspondance, tout arbre sur $[n]$ ayant $(d_1, \ldots, d_n)$ comme vecteur de degrés correspond à une fonction f satisfaisant (i) et (ii). En conclusion, nous avons une bijection entre les arbres sur $[n]$ ayant $(d_1, \ldots, d_n)$ comme vecteur de degrés et les fonctions $f : [n] \to [n]$ satisfaisant (i) et (ii). □

Remarque 1.31. Pour une autre preuve du Théorème 1.30, observer que tout sommet j apparaît exactement $d_j - 1$ fois dans le code de Prüfer d'un arbre sur $[n]$ ayant $(d_1, \ldots, d_n)$ comme vecteur de degrés. Ceci donne l'idée de compter le nombre de mots de $n-2$ symboles pris dans l'alphabet $[n]$ où le symbole j apparaît exactement $d_j - 1$ fois. On sait par ce qui précède que ce nombre est $\binom{n-2}{d_1-1,\ldots,d_n-1}$. Ce nombre est bien le nombre d'arbres à n sommets ayant $(d_1, \ldots, d_n)$ comme vecteur de degrés (bien que correct, ceci demande à être justifié).

1.9 Exercices

Exercice 1.1. Soient A et B deux ensembles finis avec $|A| = a$ et $|B| = b$ ($a, b \in \mathbb{N}$). Que valent :

(i) $|A \times B|$,

(ii) $|B^A|$ où $B^A := \{f : A \to B\}$,

(iii) $|\{f : A \to B : f \text{ est une injection de } A \text{ dans } B\}|$,

(iv) $|\mathrm{Sym}\, A|$ où $\mathrm{Sym}\, A$ est l'ensemble des permutations de A.

Exercice 1.2. Quels sont les ensembles F non vides ayant la propriété suivante :

(i) pour tout ensemble X, $|F^X| = 1$?

(ii) pour tout ensemble Y, $|Y^F| = 1$?

Exercice 1.3. Soient $f : A \to B$ et $g : B \to C$ deux fonctions. Démontrer :

(i) $g \circ f$ injective $\Rightarrow$ f injective ;

(ii) $g \circ f$ surjective $\Rightarrow$ g surjective ;

(iii) $g \circ f$ bijective $\Rightarrow$ (f injective et g surjective).

Exercice 1.4. Donner une bijection explicite entre l'ensemble des bijections de $[n]$ vers $[n]$ et l'ensemble $[n] \times [n-1] \times \cdots \times [1]$.

Exercice 1.5. Donner une preuve bijective de l'identité de somme parallèle $\binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{m}{k} = \binom{m+1}{k+1}$.

Exercice 1.6. Donner deux démonstrations de

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \,.$$

Exercice 1.7. Prouver, pour $n \in \mathbb{N}_0$,

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 \,.$$

Exercice 1.8. Qu'obtient-on comme identité sur les coefficients binomiaux en écrivant

$$(x+y)^{2n} = (x+y)^n (x+y)^n \ ?$$

Exercice 1.9. Qu'obtient-on en dérivant la formule du binôme ?

Exercice 1.10. Obtenir l'identité de symétrie à partir de la formule du binôme.

Exercice 1.11. Pour $n \geqslant 1$, que vaut la somme des coefficients binomiaux $\binom{n}{k}$ avec k pair ?

Exercice 1.12. Trouver le nombre de solutions de l'équation $x + y + z + w = 15$, dans les naturels.

Exercice 1.13. Combien l'équation

$$x + y + z + t + u = 60$$

possède-t-elle de solutions entières (x, y, z, t, u) telles que

$$x > 0 \,, \quad y \geqslant 9 \,, \quad z > -2 \,, \quad t \geqslant 0 \quad \text{et} \quad u > 10 \quad ?$$

Exercice 1.14. Trouver le nombre de solutions de l'inéquation

$$x + y + z + t \leqslant 6$$

(i) dans les naturels ;

(ii) dans les entiers > 0 ;

(iii) dans les entiers, avec comme contraintes supplémentaires $x > 2$, $y > -2$, $z > 0$ et $t > -3$.

Exercice 1.15. Combien le système d'équations

$$\begin{cases} x + y + z + t &= 415 \\ x + y + z + u &= 273 \end{cases}$$

possède-t-il de solutions (x, y, z, t, u) en entiers > 0 ?

Exercice 1.16. Combien l'inéquation

$$x + y + z + t < 100$$

possède-t-elle de solutions (x, y, z, t) en entiers > 0 ?

Exercice 1.17. Quel est le nombre de partitions de $[n]$ en classes comportant toutes exactement 2 éléments ?

Exercice 1.18. Avec les lettres du mot MISSISSIPPI, combien peut-on écrire de mots différents de 11 lettres ?

Exercice 1.19. Dans le triangle de Pascal, prouver que le produit des 6 voisins d'un coefficient binomial $\binom{n}{k}$ est toujours un carré parfait.

Exercice 1.20. Que vaut

$$\sum_{k=0}^{n} k \binom{n}{k} \quad ?$$

Exercice 1.21. Que vaut

$$\sum_{k=0}^{n} \frac{1}{k+1} \binom{n}{k} \quad ?$$

Exercice 1.22. Avec les lettres du mot

H U M U H U M U N U K U N U K U A P U A A

("poisson" en hawaïen), combien peut-on écrire de mots différents de 21 lettres ne comprenant pas deux lettres U côte à côte ?

Exercice 1.23.

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = \quad ?$$

Exercice 1.24. Si $0 \leqslant m \leqslant n$, que vaut

$$\sum_{k=m}^{n} \binom{k}{m} \binom{n}{k} \quad ?$$

(Hint : essayer une preuve bijective.)

Exercice 1.25. Si on jette simultanément n dès identiques, combien de résultats différents peut-on obtenir ? (Deux résultats sont considérés comme équivalents s'ils ont le même nombre de 1, le même nombre de 2, ..., le même nombre de 6.)

Exercice 1.26.

$$\sum_{i=0}^{n} \sum_{j=0}^{i} \binom{n}{i} \binom{i}{j} = \quad ?$$

Exercice 1.27.

$$\sum_{i=0}^{n} \binom{n+1}{i+1} (i+1) 2^i = \quad ?$$

Exercice 1.28. (Examen août 2011.) Pour des naturels n et r, on pose

$$A_r^n := \sum_{k=0}^{n} k^r \binom{n}{k} .$$

- Sur base de cette relation de récurrence, donner une formule pour A_1^n et A_2^n valable pour tout $n \in \mathbb{N}$.
- En utilisant les propriétés des coefficients binomiaux, démontrer que les nombres A_r^n vérifient la relation de récurrence $A_r^n = n(A_{r-1}^n - A_{r-1}^{n-1})$.

Exercice 1.29. (Difficile) Calculer l'inverse de la matrice $(n+1) \times (n+1)$ formée des $n+1$ premières lignes du triangle de Pascal. Si on appelle cette matrice $A = (a_{ij})$, alors $a_{ij} = \binom{i}{j}$ pour $i = 0, \ldots, n$ et $j = 0, \ldots, n$.

Exercice 1.30. Ecrire l'algorithme permettant de calculer le code de Prüfer $c = c(T)$ d'un arbre T sur $[n]$. Trouver ensuite un algorithme permettant, étant donné un code de Prüfer $c \in [n]^{n-2}$, de trouver l'arbre T correspondant. Justifier soigneusement que votre algorithme est correct.

Exercice 1.31. Vérifier que

$$\sum_{(d_1,\ldots,d_n)} \binom{n-2}{d_1 - 1, \ldots, d_n - 1} = n^{n-2}$$

où la somme est prise sur les vecteurs des degrés des arbres sur $[n]$.

Chapitre 2

Relations de récurrence

2.1 Exemples récurrents

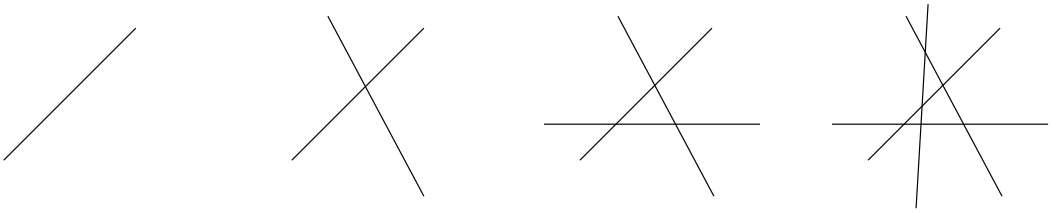
2.1.1 Nombres de régions délimitées par n droites dans le plan

Dans ce premier exemple, nous étudions le problème suivant :

Combien de régions du plan n droites (en position générale) déterminent-elles ?

Définition 2.1 (Droites en position générale)**.** Un ensemble de droites du plan est *en position générale* si toute paire de droites s'intersectent en exactement un point et tout triple de droites ont une intersection vide.

Appelons $\Phi_2(n)$ le nombre de régions du plan délimitées par n droites en position générale. Notre but est d'obtenir une formule close pour $\Phi_2(n)$. En particulier, nous allons voir que *le nombre de régions dépend uniquement du nombre de droites, et pas de l'arrangement lui-même*. Comment procéder ? Voyons tout d'abord ce que vaut $\Phi_2(n)$ pour des petites valeurs de n.



$n = 1$ $n = 2$ $n = 3$ $n = 4$

n	0	1	2	3	4	$\cdots$
$\Phi_2(n)$	1	2	4	7	11	$\cdots$

En regardant bien ces nombres, on peut observer que les différences entre deux nombres consécutifs sont très régulières : 1, 2, 3, 4, ... En extrapolant, on devine que la différence entre $\Phi_2(n)$ et $\Phi_2(n-1)$ est exactement n. Démontrons-le.

Théorème 2.2. *Pour tout $n \in \mathbb{N}$, le nombre de régions du plan délimitées par n droites en position générale ne dépend pas du choix de ces droites. En d'autres termes, $\Phi_2(n)$ est bien défini. De plus,*

$$\Phi_2(n) = \Phi_2(n-1) + n$$

pour $n \geqslant 1$, et $\Phi_2(0) = 1$.

Démonstration. Le fait que $\Phi_2(0)$ est bien défini et vaut 1 est évident. Maintenant, supposons $n \geqslant 1$ et supposons $\Phi_2(n-1)$ bien défini. Numérotons les droites de l'arrangement $D_1, \ldots, D_n$. Le nombre de régions délimitées par les droites $D_1, \ldots, D_{n-1}$ vaut $\Phi_2(n-1)$. Rajoutons la droite D_n à cet arrangement. Cette dernière droite coupe certaines des régions de l'arrangement $D_1, \ldots, D_{n-1}$ en deux. Le nombre de telles régions est égal au nombre d'intervalles de la droite D_n délimités par $D_1, \ldots, D_{n-1}$, c'est-à-dire n. Donc $\Phi_2(n)$ est bien défini et vaut $\Phi_2(n-1) + n$. □

Pour résoudre la récurrence obtenue ci-dessus pour $\Phi_2(n)$, on la déroule :

$$\begin{aligned}
\Phi_2(n) &= n + \Phi_2(n-1) \\
&= n + (n-1) + \Phi_2(n-2) \\
&\vdots \\
&= n + (n-1) + (n-2) + \cdots + 1 + \overbrace{\Phi_2(0)}^{=1} \\
&= \frac{n(n+1)}{2} + 1 \\
&= \frac{n(n-1)}{2} + n + 1 \\
&= \binom{n}{2} + \binom{n}{1} + \binom{n}{0}.
\end{aligned}$$

Il est difficile de résister à une envie de généraliser cette formule à une dimension d quelconque. Généralisons-la tout d'abord à la dimension $d = 3$. Considérons donc maintenant n plans dans l'espace (de dimension 3) en position générale.

Définition 2.3 (Plans en position générale)**.** Un ensemble de *plans* de l'espace est *en position générale* si toute paire de plans s'intersectent en une droite, tout triple de plans s'intersectent en un point et tout quadruple de plans ont une intersection vide.

Appelons $\Phi_3(n)$ le nombre de régions de l'espace délimitées par n plans (en position générale). Un raisonnement analogue à celui effectué dans la preuve du Théorème 2.2 —la seule différence est que le nombre de nouvelles régions créées par l'ajout du n-ème plan vaut le nombre de régions de ce plan délimitées pas les $n-1$ premiers plans, c'est-à-dire $\Phi_2(n-1)$— on obtient la récurrence suivante :

$$\Phi_3(n) = \Phi_3(n-1) + \Phi_2(n-1) \quad \forall n \geqslant 1; \quad \Phi_3(0) = 1\,.$$

En déroulant, on obtient une formule pour $\Phi_3(n)$:

$$\begin{aligned}
\Phi_3(n) &= \Phi_2(n-1) + \Phi_3(n-1) \\
&= \binom{n-1}{2} + \binom{n-1}{1} + \binom{n-1}{0} + \Phi_3(n-1) \\
&= \left[\binom{n-1}{2} + \binom{n-1}{1} + \binom{n-1}{0}\right] + \left[\binom{n-2}{2} + \binom{n-2}{1} + \binom{n-2}{0}\right] \\
&\quad + \ldots + \underbrace{\left[\binom{0}{2} + \binom{0}{1} + \binom{0}{0}\right]}_{\Phi_2(0)} + \underbrace{\Phi_3(0)}_{=1=\binom{n}{0}} \\
&= \binom{n}{3} + \binom{n}{2} + \binom{n}{1} + \binom{n}{0}.
\end{aligned}$$

La dernière égalité utilise (trois fois) l'identité de somme parallèle (Théorème 1.20).

Tout ceci se généralise en dimension d quelconque. Pour la récurrence :

$$\Phi_d(n) = \Phi_d(n-1) + \Phi_d(n-1) \quad \forall n \geqslant 1; \quad \Phi_d(0) = 1$$

et pour la formule :

$$\Phi_d(n) = \binom{n}{d} + \binom{n}{d-1} + \ldots + \binom{n}{1} + \binom{n}{0} .$$

2.1.2 Pavages d'un rectangle $2 \times n$

Etudions maintenant le problème suivant :

> *De combien de manières peut-on paver un rectangle* $2 \times n$ *avec des rectangles* 1×2 *(dits "horizontaux") et* 2×1 *(dits "verticaux") ?*

Notons ce nombre p_n (pour $n \geqslant 0$). On obtient facilement une récurrence pour p_n. En effet, considérons un pavage quelconque d'un rectangle $2 \times n$ avec $n \geqslant 3$. De deux choses l'une :

a) soit le rectangle dans le coin inférieur gauche est vertical ;

b) soit le rectangle dans le coin inférieur gauche est horizontal.

Dans le cas a) on peut compléter le pavage par n'importe quel pavage d'un rectangle $2 \times (n-1)$. Dans le cas b) le rectangle situé juste au-dessus est également horizontal et on peut compléter le pavage par n'importe quel pavage d'un rectangle $2 \times (n-2)$. De plus, il est évident que $p_1 = 1$ et $p_2 = 2$. En résumé :

$$p_n = p_{n-1} + p_{n-2} \quad \forall n \geqslant 3; \quad p_1 = 1;\ p_2 = 2 .$$

Pour les petites valeurs de n, on trouve :

n	1	2	3	4	5	$\cdots$
p_n	1	2	3	5	8	$\cdots$

Ce sont des nombres de Fibonacci. Plus précisément, p_n est égal au $(n+1)$-ème nombre de Fibonacci F_{n+1}.

Définition 2.4 (Suite de Fibonacci)**.** La suite des *nombres de Fibonacci* (~ 1200) est l'unique suite $(F_n)_{n \in \mathbb{N}}$ solution de la récurrence :

$$F_n = F_{n-1} + F_{n-2} \quad \forall n \geqslant 2; \quad F_0 = 0;\ F_1 = 1 .$$

Nous allons maintenant trouver une formule explicite pour le n-ème nombre de Fibonacci F_n. Le lecteur familier avec les méthodes de résolution d'équations différentielles linéaires à coefficients constants devrait facilement s'y retrouver car ces équations se résolvent de la même manière que les équations de récurrence linéaires à coefficients constants, comme par exemple celle qui définit la suite de Fibonacci.

On cherche des solutions de la forme $F_n = \beta^n$ pour certains $\beta \in \mathbb{R} \setminus \{0\}$. Réécrivons l'équation $F_n = F_{n-1} + F_{n-2}$ en remplaçant F_n par β^n :

$$\begin{array}{rrcl} & \beta^n & = & \beta^{n-1} + \beta^{n-2} \quad \forall n \geqslant 2 \\ \overset{\beta \neq 0}{\Longleftrightarrow} & \beta^2 & = & \beta + 1 \\ \Longleftrightarrow & \beta & = & \frac{1 \pm \sqrt{5}}{2} . \end{array}$$

Définition 2.5 (Nombre d'or)**.** Posons $\varphi := \frac{1+\sqrt{5}}{2}$ et $\bar{\varphi} := \frac{1-\sqrt{5}}{2}$. L'irrationnel φ est le *nombre d'or*. L'irrationnel $\bar{\varphi}$ est le *conjugué* du nombre d'or φ.

Par ce qui précède, $(\varphi^n)_{n\in\mathbb{N}}$ et $(\bar{\varphi}^n)_{n\in\mathbb{N}}$ sont deux solutions de $F_n = F_{n-1} + F_{n-2}$. Par linéarité, on voit rapidement que toute suite de la forme

$$F_n = \lambda_1 \varphi^n + \lambda_2 \bar{\varphi}^n \quad \forall n \in \mathbb{N} \tag{2.1}$$

est également solution, pour tout choix de constantes $\lambda_1, \lambda_2 \in \mathbb{R}$. Ceci est dû au fait que l'ensemble des suites solutions de notre équation de récurrence forme un sous-espace vectoriel de l'espace vectoriel $\mathbb{R}^{\mathbb{N}}$ des suites réelles. Or la dimension de ce sous-espace est *exactement* 2. Intuitivement, le choix des conditions initiales F_0 et F_1 donne deux degrés de liberté, et tout est déterminé quand on connaît F_0 et F_1. Les suites $(\varphi^n)_{n\in\mathbb{N}}$ et $(\bar{\varphi}^n)_{n\in\mathbb{N}}$ étant linéairement indépendantes (voyez-vous pourquoi ?), elles forment une *base* de l'espace des solutions. Dès lors, toute suite solution est de la forme (2.1).

Théorème 2.6. *Pour tout $n \in \mathbb{N}$,*

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

Démonstration. Par ce qui précède, il existe des constantes $\lambda_1, \lambda_2 \in \mathbb{R}$ telles que F_n est donné par (2.1). En imposant les conditions initiales $F_0 = 0$ et $F_1 = 1$, on trouve

$$\begin{aligned} n = 0 : \qquad & 0 = F_0 = \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right)^0 + \lambda_2 \left(\frac{1-\sqrt{5}}{2}\right)^0 \\ n = 1 : \qquad & 1 = F_1 = \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 + \lambda_2 \left(\frac{1-\sqrt{5}}{2}\right)^1 . \end{aligned}$$

Ce système de deux équations à deux inconnues s'écrit :

$$\left\{ \begin{array}{rcl} \lambda_1 + \lambda_2 & = & 0 \\ \left(\frac{1+\sqrt{5}}{2}\right)\lambda_1 + \left(\frac{1-\sqrt{5}}{2}\right)\lambda_2 & = & 1 \end{array} \right.$$

En résolvant ce système, on trouve :

$$\left\{ \begin{array}{rcl} \lambda_1 & = & \frac{1}{\sqrt{5}} \\ \lambda_2 & = & \frac{-1}{\sqrt{5}} . \end{array} \right.$$

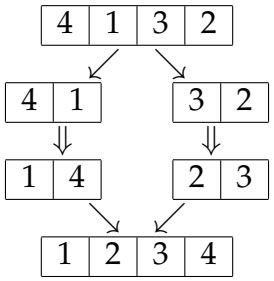
□

Remarque 2.7. Etant donné que $\bar{\varphi} = -0,618\ldots$ est de valeur absolue strictement plus petite que 1, on a $\lim_{n\to\infty} \bar{\varphi}^n$. Donc, le n-ème nombre de Fibonacci F_n est simplement l'entier le plus proche de $\frac{1}{\sqrt{5}}\varphi^n$ (pour n suffisamment grand).

2.1.3 Tri fusion

Le *tri fusion* (*Mergesort*) est un algorithme bien connu pour trier N nombres (ou de manière plus générale, N objets totalement ordonnés). Etant donné un vecteur de taille N, cet algorithme le partitionne en deux vecteurs de tailles $\lceil N/2 \rceil$ et $\lfloor N/2 \rfloor$, puis s'appelle récursivement sur chacun de ces deux vecteurs, et enfin fusionne les vecteurs résultants. Nous étudierons une suite C_N qui donne le nombre total de *copies* effectuées par le tri fusion pour trier un vecteur de taille N (c'est aussi une majoration sur le nombre de comparaisons effectuées).

Exemple 2.8. Voyons un exemple pour $N = 4$.



Pour le moment, on prend $N = 2^n$ ($n \geqslant 0$). Nous verrons le cas général plus tard. Etant donné la structure récursive de l'algorithme, nous pouvons écrire

$$C_N = C_{\lceil N/2 \rceil} + C_{\lfloor N/2 \rfloor} + N \quad \forall N \geqslant 2; \quad C_1 = 0\,.$$

En effet, l'algorithme copie exactement N nombres quand il fusionne les deux vecteurs de taille $\lfloor N/2 \rfloor$ et $\lceil N/2 \rceil$, les autres copies sont dûes aux appels récursifs. Pour $N = 2^n$, les plancher et plafond disparaissent :

$$C_{2^n} = 2C_{2^{n-1}} + 2^n \quad \forall n \geqslant 1; \quad C_{2^0} = 0\,.$$

Après division par 2^n :

$$\frac{C_{2^n}}{2^n} = \frac{C_{2^{n-1}}}{2^{n-1}} + 1 \quad \forall n \geqslant 1; \quad \frac{C_{2^0}}{2^0} = 0\,.$$

Après un moment de réflexion, on voit qu'il faut changer de variables et poser $a_n := \frac{C_{2^n}}{2^n}$. Résoudre la récurrence dans les nouvelles variables est un jeu d'enfant :

$$\begin{aligned} a_n &= 1 + a_{n-1} \\ &= 1 + 1 + a_{n-2} \\ &= \cdots \\ &= \underbrace{1+1+1+1+\ldots+1}_{n \text{ fois}} + \underbrace{a_0}_{=0} \\ &= n \end{aligned}$$

En revenant aux variables originales, on a $C_{2^n} = 2^n a_n = 2^n n$. Etant donné que $N = 2^n$, on a $n = \log_2 N$ et on obtient le résultat suivant.

Proposition 2.9. *Le nombre de copies effectuées par le tri fusion sur un vecteur de taille $N = 2^n$ est*

$$C_N = N \log_2 N\,.$$

2.2 Récurrences linéaires

Après les exemples de la section précédente, nous allons développer de manière théorique des méthodes de résolution pour des équations de récurrence qui généralisent, entre autres, l'équation définissant la suite de Fibonacci.

2.2.1 Récurrences linéaires du premier ordre

Théorème 2.10. *La récurrence*

$$x_n = c_n x_{n-1} + d_n \quad \forall n \geqslant 1; \quad x_0 = 0$$

a pour solution explicite

$$x_n = \sum_{i=1}^{n} d_i \prod_{j=i+1}^{n} c_j = d_n + d_{n-1}c_n + d_{n-2}c_{n-1}c_n + \cdots + d_1 c_2 \cdots c_n.$$

Démonstration. Par récurrence sur n. C'est vrai pour $n = 0$ (car une somme vide est par définition nulle). Supposons maintenant $n > 0$ et $x_{n-1} = \sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n-1} c_j$. Alors

$$\begin{aligned} x_n &= c_n x_{n-1} + d_n \\ &= c_n \sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n-1} c_j + d_n \\ &= \sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n} c_j + d_n \\ &= \sum_{i=1}^{n} d_i \prod_{j=i+1}^{n} c_j \,. \end{aligned}$$

□

2.2.2 Récurrences linéaires homogènes à coefficients constants

L'équation de Fibonacci $F_n = F_{n-1} + F_{n-2}$ est un exemple très simple de récurrence linéaire à coefficients constants (RLCC) homogène. En général, une RLCC homogène s'écrit :

$$x_n = c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \cdots + c_0 x_{n-d} \quad \forall n \geqslant d \,,$$

ou encore

$$-x_n + c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \cdots + c_0 x_{n-d} = 0 \quad \forall n \geqslant d \,. \tag{2.2}$$

Les nombres $c_0, c_1, \ldots, c_d$ sont des constantes. Pour des raisons qui seront évidentes plus tard, on va prendre $c_0, c_1, \ldots, c_d \in \mathbb{C}$ (même si en pratique, les coefficients seront entiers). Si $c_0 \neq 0$, l'*ordre* d'une telle récurrence est d.

Définition 2.11 (Polynôme caractéristique)**.** Le *polynôme caractéristique* de la RLCC (2.2) est

$$p(t) := -t^d + c_{d-1}t^{d-1} + c_{d-2}t^{d-2} + \cdots + c_0 = \sum_{i=0}^{d} c_i t^i \,,$$

où $c_d := -1$.

Notre objectif est de comprendre l'ensemble des soutions des RLCC, c'est-à-dire l'ensemble des suites $(x_n)_{n\in\mathbb{N}} \in \mathbb{C}^{\mathbb{N}}$ qui satisfont (2.2). Nous verrons qu'il est possible d'écrire une formule close donnant toutes les solutions de (2.2).

Théorème 2.12. *Notons S l'ensemble des solutions de la RLCC* (2.2)*. Alors :*

(i) S est un sous-espace de $\mathbb{C}^{\mathbb{N}}$*,*

(ii) $\dim(S) = d$*.*

Démonstration. (i) En effet, si $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont solutions et $\lambda, \mu \in \mathbb{C}$, alors la suite $(z_n)_{n\in\mathbb{N}}$ définie par

$$z_n := \lambda x_n + \mu y_n \qquad \forall n \in \mathbb{N}$$

satisfait, pour $n \geqslant d$:

$$\begin{aligned} z_n &= \lambda x_n + \mu y_n \\ &= \lambda(c_{d-1}x_{n-1} + \cdots + c_0 x_{n-d}) + \mu(c_{d-1}y_{n-1} + \cdots + c_0 y_{n-d}) \\ &= c_{d-1}(\lambda x_{n-1} + \mu y_{n-1}) + \cdots + c_0(\lambda x_{n-d} + \mu y_{n-d}) \\ &= c_{d-1}z_{n-1} + \cdots + c_0 z_{n-d}\,. \end{aligned}$$

(ii) Considérons l'application linéaire

$$A : S \to \mathbb{C}^d : (x_n)_{n\in\mathbb{N}} \mapsto (x_0, \ldots, x_{d-1})\,.$$

Alors A est injective car le noyau $\ker(A) := \{x \in S \mid A(x) = 0\}$ de A est l'ensemble des suites solutions dont les d premières valeurs sont nulles. Par (2.2), la $(d+1)$-ème valeur d'une telle suite est également nulle, etc… Le noyau de A comporte donc une seule suite, la suite nulle. Ceci implique que A est injective car si $x = (x_n)_{n\in\mathbb{N}}$ et $y = (y_n)_{n\in\mathbb{N}}$ sont deux suites solution, alors

$$A(x) = A(y) \Longrightarrow A(x-y) = 0 \Longrightarrow x - y = 0 \Longrightarrow x = y\,.$$

De plus, A est surjective car pour tout choix de d conditions initiales $x_0, \ldots, x_{d-1}$ il existe une (et une seule) suite solution commençant par ces valeurs. Par conséquent, A est une application linéaire bijective, c'est-à-dire un *isomorphisme* d'espaces vectoriels. En particulier, $\dim(S) = \dim(\mathbb{C}^d) = d$. □

Définition 2.13 (Multiplicité)**.** Pour rappel, un nombre complexe $a \in \mathbb{C}$ est *une racine de multiplicité* $m = m(a)$ d'un polynôme complexe $p(t) \in \mathbb{C}[t]$ si $p(t)$ est divisible par $(t-a)^m$, mais pas par $(t-a)^{m+1}$.

Lemme 2.14. *Soit* $p(t) \in \mathbb{C}[t]$ *un polynôme complexe de degré* $d \geqslant 1$*. Un nombre complexe a est une racine de multiplicité* $m = m(a)$ *du polynôme* $p(t)$ *si et seulement si* $p(a) = \frac{\mathrm{d}p}{\mathrm{d}t}(a) = \cdots = \frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a) = 0$ *et* $\frac{\mathrm{d}^m p}{\mathrm{d}t^m}(a) \neq 0$*.*

Démonstration. Par la formule de Taylor (comme $p(t)$ est un polynôme de degré d il n'y a pas de reste), on a :

$$\begin{aligned} p(t) &= p(a) + \frac{\mathrm{d}p}{\mathrm{d}t}(a)(t-a) + \frac{1}{2}\frac{\mathrm{d}^2p}{\mathrm{d}t^2}(a)(t-a)^2 + \cdots + \frac{1}{(m-1)!}\frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a)(t-a)^{m-1} \\ &\quad + \frac{1}{m!}\frac{\mathrm{d}^m p}{\mathrm{d}t^m}(a)(t-a)^m + \cdots + \frac{1}{d!}\frac{\mathrm{d}^d p}{\mathrm{d}t^d}(a)(t-a)^d \,. \end{aligned}$$

Si $p(a) = \frac{\mathrm{d}p}{\mathrm{d}t}(a) = \cdots = \frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a)$ et $\frac{\mathrm{d}^m p}{\mathrm{d}t^m}(a) \neq 0$ alors clairement $p(t)$ est divisible par $(t-a)^m$ mais pas par $(t-a)^{m+1}$, donc a est une racine de multiplicité m. Conversément, si a est une racine de multiplicité m alors $p(t)$ est divisible par $(t-a)^m$ mais pas par $(t-a)^{m+1}$ et on doit nécessairement avoir $p(a) = 0$, puis $\frac{\mathrm{d}p}{\mathrm{d}t}(a) = 0$, …, puis $\frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a) = 0$ et enfin $\frac{\mathrm{d}^m p}{\mathrm{d}t^m}(a) \neq 0$. □

Lemme 2.15. *Pour tout entier $j \geqslant 1$, il existe des coefficients entiers $\alpha_1, \alpha_2, \ldots, \alpha_j$ tels que*

$$i^j = \alpha_1\, i + \alpha_2\, i(i-1) + \cdots + \alpha_j\, i(i-1)\cdots(i-j+1) = \sum_{k=1}^{j} \alpha_k i(i-1)\cdots(i-k+1)\,.$$

Démonstration. Par récurrence sur j. Pour $j = 1$, on a $i^1 = i$ donc on peut prendre $\alpha_1 = 1$. Notons aussi que, pour $j = 2$, on a $i^2 = i + i(i-1)$ donc on peut prendre $\alpha_1 = \alpha_2 = 1$ dans ce cas. Supposons maintenant qu'il existe des coefficients entiers $\alpha_1, \alpha_2, \ldots, \alpha_j$ (avec $j \geqslant 2$) tels que

$$i^j = \alpha_1\, i + \alpha_2\, i(i-1) + \cdots + \alpha_j\, i(i-1)\cdots(i-j+1) = \sum_{k=1}^{j} \alpha_k i(i-1)\cdots(i-k+1)\,.$$

Alors

$$\begin{aligned} i^{j+1} &= i \cdot i^j \\ &= i \cdot (\alpha_1\, i + \alpha_2\, i(i-1) + \cdots + \alpha_j\, i(i-1)\cdots(i-j+1)) \\ &= \alpha_1\, i^2 + \alpha_2\, i^2(i-1) + \cdots + \alpha_j\, i^2(i-1)\cdots(i-j+1) \\ &= \alpha_1\,(i + i(i-1)) + \alpha_2\,(i(i-1))(i-1) + \cdots + \alpha_j\,(i + i(i-1))(i-1)\cdots(i-j+1) \\ &= \sum_{k=1}^{j} \alpha_k i(i-1)\cdots(i-k+1) + \alpha_1 i(i-1) + \sum_{k=2}^{j} \alpha_k i(i-1)^2\cdots(i-k+1) \end{aligned}$$

On peut ensuite remplacer $(i-1)^2$ dans la dernière somme par $(i-1) + (i-1)(i-2)$, etc… En continuant le calcul, on obtient en définitive une expression de i^j comme combinaison linéaire à coefficients entiers de i, $i(i-1)$, $i(i-1)(i-2)$, …, $i(i-1)\cdots(i-k)$. □

Lemme 2.16. *Si $a \in \mathbb{C}$ est une racine de multiplicité $m \geqslant 1$ du polynôme $\sum_{i=0}^{d} c_i t^i \in \mathbb{C}[t]$ de degré d, alors*

$$\sum_{i=0}^{d} c_i i^j a^i = 0$$

pour $j \in \{0, \ldots, m-1\}$ et

$$\sum_{i=0}^{d} c_i i^m a^i \neq 0 \,.$$

Démonstration. Par le Lemme 2.15, on a

$$\begin{aligned}
\sum_{i=0}^{d} c_i i^j a^i &= \sum_{i=0}^{d} c_i \left(\sum_{k=1}^{j} \alpha_k \, i(i-1)\cdots(i-k+1) \right) a^i \\
&= \sum_{k=1}^{j} \alpha_k \left(\sum_{i=0}^{d} c_i \, i(i-1)\cdots(i-k+1)\, a^i \right) \\
&= \sum_{k=1}^{j} \alpha_k \, p^{\underline{k}}(a) \,.
\end{aligned}$$

Par le Lemme 2.14, cette dernière expression est nulle quand $j < m$ et non nulle quand $j = m$ (notons qu'on a toujours $\alpha_j = 1$). □

Théorème 2.17 (Récurrences linéaires homogènes à coefficients constants)**.** *Considérons la RLCC homogène d'ordre $d \geqslant 1$:*

$$-x_n + c_{d-1} x_{n-1} + c_{d-2} x_{n-2} + \cdots + c_0 x_{n-d} = 0 \quad \forall n \geqslant d \,.$$

où $c_0, \ldots, c_{d-1} \in \mathbb{C}$ et $c_0 \neq 0$. Notons $p(t) := \sum_{i=0}^{d} c_i t^i \in \mathbb{C}[t]$ son polynôme caractéristique*, où $c_d := -1$. Toute solution de cette relation de récurrence est une combinaison linéaire des d suites de la forme $(n^j \beta^n)_{n \in \mathbb{N}}$, où β est une racine de $p(t)$ et $j \in \{0, 1, \ldots, m(\beta) - 1\}$, c.-à-d. j est un naturel strictement inférieur à la multiplicité de β.*

Démonstration. Soit S l'ensemble des suites solutions de l'équation. Par le Théorème 2.12, S est un espace vectoriel sur le corps des complexes, de dimension d. Considérons maintenant une racine β de $p(t)$, de multiplicité $m = m(\beta) \geqslant 1$. Etant donné que $c_0 \neq 0$, on a $\beta \neq 0$. La suite $(n^j \beta^n)_{n \in \mathbb{N}}$ est solution de l'équation si et seulement si, pour tout naturel $n \geqslant d$,

$$\begin{aligned}
\sum_{i=0}^{d} c_i (i + (n-d))^j \beta^{i+(n-d)} = 0 \quad &\overset{\beta \neq 0}{\iff} \quad \sum_{i=0}^{d} c_i (i + (n-d))^j \beta^i = 0 \\
&\iff \quad \sum_{i=0}^{d} c_i \left(\sum_{k=0}^{j} \binom{j}{k} i^{j-k} (n-d)^k \right) \beta^i = 0 \\
&\iff \quad \sum_{k=0}^{j} \binom{j}{k} (n-d)^k \left(\sum_{i=0}^{d} c_i i^{j-k} \beta^i \right) = 0 \,.
\end{aligned}$$

Par le Lemme 3, $\sum_{i=0}^{d} c_i i^{j-k} \beta^i = 0$ dès que $j < m$. Donc en particulier on voit que la suite $(n^j \beta^n)_{n\in\mathbb{N}}$ est solution pour $j \in \{0, \ldots, m-1\}$. On voit aussi que pour $j = m$, la suite n'est pas une solution (ne soyons pas trop gourmand !).

Etant donné que chaque racine β du polynôme caractéristique, de multiplicité $m(\beta)$, donne $m(\beta)$ solutions de la forme $(n^j \beta^n)_{n\in\mathbb{N}}$, et que $\sum_{\beta \text{ racine}} m(\beta) = d$ par le Théorème Fondamental de l'Algèbre (tout polynôme $p(t) \in \mathbb{C}[t]$ de degré d a exactement d racines, en tenant compte des multiplicités), on a exactement d suites solutions de la forme $(n^j \beta^n)_{n\in\mathbb{N}}$ avec β racine du polynôme caractéristique $p(t)$ et $j \in \{0, \ldots, m(\beta) - 1\}$. Pour conclure, il suffit de démontrer que ces d suites sont linéairement indépendantes (ceci est un exercice non trivial laissé au lecteur). □

Par le théorème précédent, la solution générale d'une RLCC homogène peut s'écrire

$$x_n = \sum_{\beta \text{ racine}} \sum_{j=0}^{m(\beta)-1} \lambda_{\beta,j}\, n^j \beta^n$$

où les $\lambda_{\beta,j}$ sont des coefficients complexes déterminés dès que l'on possède d conditions initiales $x_0, \ldots, x_{d-1}$. L'apparition des nombres complexes dans l'analyse de suites entières ne doit pas causer de panique ! Tout comme la formule qui donne les nombres de Fibonacci fait intervenir des irrationnels, alors que ceux-ci sont entiers, une RLCC homogène à coefficients entiers avec des conditions initiales entières aura pour solution une suite entière même si des nombres complexes interviennent dans la formule définissant la suite.

Exemple 2.18. $x_n + x_{n-1} + x_{n-2} = 0$ pour $n \geqslant 2$ avec $x_0 = 0$ et $x_1 = 1$. La solution est

$$x_n = \frac{i}{\sqrt{3}} \left(\left(\frac{-1 - \sqrt{3}i}{2} \right)^n - \left(\frac{-1 + \sqrt{3}i}{2} \right)^n \right) .$$

Horreur ? Non, la suite est toujours à valeurs entières. Si on s'interdisait d'utiliser les complexes, on se priverait d'une belle formule !

2.2.3 Récurrences linéaires à coefficients constants générales

L'étude des RLCC générales (c'est-à-dire, non nécessairement homogènes), du type

$$-x_n + c_{d-1} x_{n-1} + c_{d-2} x_{n-2} + \cdots + c_0 x_{n-d} = a_n \quad \forall n \geqslant d$$

où $(a_n)_{n\in\mathbb{N}}$ est une suite donnée, commence par l'étude de la *RLCC homogène associée*

$$-x_n + c_{d-1} x_{n-1} + c_{d-2} x_{n-2} + \cdots + c_0 x_{n-d} = 0 \quad \forall n \geqslant d\,.$$

Si on appelle S^{EHA} l'ensemble des solutions de cette RLCC homogène, et S l'ensemble des solutions de la RLCC de départ on a que S est simplement un translaté de S^{EHA}. Dès qu'on connaît une solution $(x_n^{SP})_{n\in\mathbb{N}}$ de la RLCC de départ, on peut écrire $S = S^{EHA} + x^{SP}$. En d'autres termes, la solution générale de l'équation de départ s'exprime comme

$$x_n = x_n^{EHA} + x_n^{SP} \quad \forall n \in \mathbb{N}$$

où $(x_n^{EHA})_{n\in\mathbb{N}}$ est la solution générale de la RLCC homogène associée et $(x_n^{SP})_{n\in\mathbb{N}}$ est la solution particulière que l'on s'est donnée (voir les séances d'exercices pour les exemples).

2.3 Récurrences diviser-pour-régner ("divide-and-conquer")

Pour rappel, on a vu que pour $N = 2^n$, la solution de

$$C_N = C_{\lceil N/2 \rceil} + C_{\lfloor N/2 \rfloor} + N \quad \forall N \geqslant 2; \quad C_1 = 0$$

est $C_N = N \lg N$. C'est un exemple de récurrence diviser-pour-régner ("divide-and-conquer"). Celles-ci sont

– très importantes en analyse d'algorithmes ;

– sujettes à des comportements oscillatoires / fractals dûs à la présence de $\lfloor \ldots \rfloor$ et $\lceil \ldots \rceil$.

On se contentera le plus souvent de déterminer le comportement asymptotique des solutions.

2.3.1 Recherche binaire

Pour localiser un nombre x dans un vecteur trié de taille N, l'algorithme de *recherche binaire* compare x au $\lceil N/2 \rceil$-ème élément du vecteur (appelé *pivot*). Si x est égal au pivot, l'algorithme s'arrête en ayant localisé x. Si x est plus petit que le pivot, l'algorithme s'appelle récursivement sur le sous-vecteur constitué des éléments en positions 1 jusque $\lceil N/2 \rceil - 1$. Si x est plus grand que le pivot, l'algorithme s'appelle récursivement sur le sous-vecteur constitué des éléments en positions $\lceil N/2 \rceil + 1$ jusque N.

Théorème 2.19. *Le nombre de comparaisons effectuées au pire des cas par une recherche binaire dans un vecteur trié de taille N est exactement le nombre de bits dans la représentation binaire de N, c'est-à-dire* $\lfloor \lg N \rfloor + 1$. *Ces quantités sont solutions de la récurrence*

$$B_N = B_{\lfloor N/2 \rfloor} + 1 \quad \forall N \geqslant 2$$

avec $B_1 = 1$.

Démonstration. Pour N pair, aussi bien que pour N impair, la plus grande des deux parties après comparaison avec l'élément médian a pour taille exactement $\lfloor N/2 \rfloor$. Si on appelle B_N le nombre de comparaisons effectuées au pire des cas par une recherche binaire dans un vecteur trié de taille N, alors on voit que

$$B_N = B_{\lfloor N/2 \rfloor} + 1 \quad \forall N \geqslant 2\,,$$

et $B_1 = 1$. C'est exactement le nombre de bits dans la représentation binaire de N car $\lfloor N/2 \rfloor$ est le naturel obtenu en décalant N d'un bit vers la droite, et le nombre 1 comporte exactement un bit dans sa représentation binaire. □

2.3.2 Retour au tri fusion

Rappelons la récurrence donnant le nombre de copies effectuées par le tri fusion :

$$C_N = C_{\lceil N/2 \rceil} + C_{\lfloor N/2 \rfloor} + N \quad \forall N \geqslant 2; \quad C_1 = 0\,.$$

Ecrivons l'équation de récurrence pour N et puis pour $N+1$, puis soustrayons :

$$\begin{array}{rcl} C_{N+1} & = & C_{\lfloor (N+1)/2 \rfloor} + C_{\lceil (N+1)/2 \rceil} + N + 1 \\ C_N & = & C_{\lfloor N/2 \rfloor} + C_{\lceil N/2 \rceil} + N \\ \hline C_{N+1} - C_N & = & C_{\lfloor (N+1)/2 \rfloor} - C_{\lceil N/2 \rceil} + C_{\lceil (N+1)/2 \rceil} - C_{\lceil N/2 \rceil} + 1 \\ & = & C_{\lceil (N+1)/2 \rceil} - C_{\lfloor N/2 \lfloor} + 1 \\ & = & C_{\lfloor N/2 \rfloor + 1} + C_{\lfloor N/2 \rfloor} + 1 \end{array}$$

L'avant-dernière égalité résulte du fait que $\lceil (N+1)/2 \rceil = \lfloor N/2 \rfloor$ pour tout entier N. La dernière égalité est une conséquence de l'identité $\lceil (N+1)/2 \rceil = \lfloor N/2 \rfloor + 1$, valable pour tout entier N.

En posant $D_N := C_{N+1} - C_N$, on obtient la récurrence $D_N = D_{\lfloor N/2 \rfloor} + 1$ pour $N \geqslant 2$ et $D_1 = C_2 - C_1 = 2 - 0 = 2$. Donc on obtient $D_N = \lfloor \lg N \rfloor + 2$ pour $N \geqslant 1$. Par conséquent,

$$\begin{array}{rcl} C_N & = & C_N - 0 \\ & = & C_N - C_1 \\ & = & (C_N - C_{N-1}) + (C_{N-1} - C_{N-2}) + \cdots + (C_2 - C_1) \\ & = & D_{N-1} + D_{N-2} + \cdots + D_1 \\ & = & \displaystyle\sum_{k=1}^{N-1} (\lfloor \lg k \rfloor + 2) \\ & = & \displaystyle (N-1) + \sum_{k=1}^{N-1} (\lfloor \lg k \rfloor + 1) \, . \end{array}$$

Cette dernière quantité est $N-1$ plus le nombre total de bits dans les représentations binaires des nombres entiers de 1 à $N-1$.

Exemple 2.20. Par exemple, $C_8 = 7 + 21 = 28$ car le nombre total de bits écrits quand on écrit les représentations binaires de 1, 2, …, 8 est exactement 21.

$$\begin{array}{r} 1 \\ 10 \\ 11 \\ 100 \\ 101 \\ 110 \\ 111 \\ 1000 \end{array} \longrightarrow 21 \text{ bits}$$

Théorème 2.21. *Le nombre de copies effectuées par le tri fusion pour un vecteur de taille N est exactement*

$$C_N = N\lfloor \lg N \rfloor + 2N - 2^{\lfloor \lg N \rfloor + 1} \, .$$

Ce nombre est une majoration sur le nombre de comparaisons *effectuées par le tri fusion.*

Démonstration.
- Les nombres $1, \ldots, N-1$ ont $\geqslant 1$ bit dans leur représentation binaire.
- Parmi ceux-ci, seuls les nombres $2, \ldots, N-1$ ont $\geqslant 2$ bits dans leur repŕesentation binaire.

– Parmi ceux-ci, seuls les nombres 4, …, $N-1$ ont $\geqslant 3$ bits dans leur représentation binaire.
– Etc…

On en déduit :

$$\begin{aligned} C_N &= (N-1)+(N-1)+(N-2)+(N-4)+\cdots+(N-2^{\lfloor \lg N \rfloor}) \\ &= (N-1)+(N-2^0)+(N-2^1)+(N-2^2)+\cdots+(N-2^{\lfloor \lg N \rfloor}) \\ &= (N-1)+N(\lfloor \lg N \rfloor+1)-(2^0+2^1+2^2+\cdots+2^{\lfloor \lg N \rfloor}) \\ &= N\lfloor \lg N \rfloor + 2N - 2^{\lfloor \lg N \rfloor+1}\,. \end{aligned}$$

□

2.3.3 Rappels sur les comportements asymptotiques

Considérons des fonctions $f, g : \mathbb{N} \to \mathbb{R}_+$ s'annulant en un nombre fini de valeurs. Alors on écrit

– $f \sim g$ si $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$, on dit alors que f et g sont *asymptotiquement équivalentes* ;
– $f = O(g)$ s'il existe une constante $C > 0$ et $n_0 \in \mathbb{N}$ tels que $f(n) \leqslant Cg(n)$ pour $n \geqslant n_0$;
– $f = o(g)$ si $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$;
– $g = \Omega(f)$ si $f = O(g)$;
– $g = \omega(f)$ si $f = o(g)$;
– $f = \Theta(g)$ si $f = O(g)$ et $g = O(f)$, on dit alors que f et g ont même *comportement asymptotique*.

Exemple 2.22. Dans la liste des fonctions suivantes, chacune des fonctions est un $o(\cdot)$, et donc un $O(\cdot)$, de la précédente :

$$n^n,\ 2^n,\ n^2,\ n,\ \sqrt{n},\ \log^2 n,\ \log n,\ \log\log n\,.$$

De plus, $n^n = \omega(2^{\log^2 n})$ et également $2^n = \omega(2^{\log^2 n})$.

2.3.4 Récurrences diviser-pour-régner générales

En analyse d'algorithmes, on cherche souvent à majorer le coût en temps (et parfois aussi en espace) d'un algorithme qui résout un problème de taille N en

– produisant α sous-problèmes de tailles $\lfloor N/\beta \rfloor$ ou $\lceil N/\beta \rceil$;
– résolvant ces sous-problèmes de manière récursive ;
– recombinant les solutions des sous-problèmes pour trouver une solution du problème original.

Le coût de construction des α sous-problèmes et de recombinaison des solutions correspondantes est majoré par une certaine fonction $f(N)$. On veut étudier la récurrence

$$a_N = \alpha a_{N/\beta} + f(N) \quad \forall N \in \mathbb{N}\,, \tag{2.3}$$

où N/β doit être interpreté tantôt comme $\lfloor N/\beta \rfloor$, tantôt comme $\lceil N/\beta \rceil$. La récurrence pour le tri fusion est un exemple où $\alpha = 2$, $\beta = 2$ et $f(N) = N$. La recherche binaire est un autre exemple, cette fois avec $\alpha = 1$, $\beta = 2$ et $f(N) = 1$.

Pour commencer, étudions l'équation fonctionnelle :

$$a(x) = \alpha a(x/\beta) + x \quad \forall x > 1; \quad a(x) = 0 \quad \forall x \leqslant 1\,. \tag{2.4}$$

Ici $\alpha, \beta \in \mathbb{R}$ sont tels que $\alpha > 0$ et $\beta > 1$.

Théorème 2.23. *Si la fonction $a : \mathbb{R}_+ \to \mathbb{R}_+$ est une solution de* (2.4)*, alors :*

Cas 1. Si $\alpha > \beta$, alors $a(x) = \Theta(x^{\log_\beta \alpha})$

Cas 2. Si $\alpha = \beta$, alors $a(x) \sim x \log_\beta x = \Theta(x \log_2 x)$

Cas 3. Si $\alpha < \beta$, alors $a(x) \sim \frac{\beta}{\beta-\alpha} x = \Theta(x)$

Démonstration. En déroulant, on trouve

$$\begin{aligned} a(x) &= x + \alpha a(x/\beta) \\ &= x + \frac{\alpha}{\beta} x + \alpha^2 a(x/\beta^2) \\ &= \dots \\ &= x\left(1 + \frac{\alpha}{\beta} + \frac{\alpha^2}{\beta^2} + \cdots + \frac{\alpha^{t-1}}{\beta^{t-1}}\right) \end{aligned}$$

pour $t := \lceil \log_\beta x \rceil$.

Cas 3 ($\alpha < \beta$). Dans ce cas, on a $\alpha/\beta < 1$ et en particulier $\alpha/\beta \neq 1$. On peut donc écrire

$$a(x) = \frac{1 - \alpha^t/\beta^t}{1 - \alpha/\beta} x \,.$$

Dans cette expression, $\alpha^t/\beta^t = (\alpha/\beta)^t$ tend vers 0 quand t tend vers $+\infty$. Quand x tend vers $+\infty$, alors $t = \lceil \log_\beta x \rceil$ aussi. Donc on trouve $a(x) \sim \frac{1}{1-\alpha/\beta} x = \frac{\beta}{\alpha-\beta} x = \Theta(x)$.

Cas 2 ($\alpha = \beta$). Dans ce cas, on a

$$a(x) = (\underbrace{1 + 1 + \ldots + 1}_{t \text{ termes}})x = t\,x = \lceil \log_\beta x \rceil x$$

et alors $a(x) \sim x \log_\beta x = \Theta(x \log_2 x)$.

Cas 1 ($\alpha > \beta$). Alors

$$\begin{aligned} a(x) &= \frac{1 - \alpha^t/\beta^t}{1 - \alpha/\beta} x \\ &= \frac{\alpha^t}{\beta^t} \frac{\beta^t/\alpha^t - 1}{1 - \alpha/\beta} x \\ &= \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x} \left(\frac{\alpha}{\beta}\right)^{\log_\beta x} \frac{\beta^t/\alpha^t - 1}{1 - \alpha/\beta} x \\ &= \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x} \frac{x^{\log_\beta \alpha}}{x} \frac{\beta^t/\alpha^t - 1}{1 - \alpha/\beta} x \\ &\sim \frac{\beta}{\beta - \alpha} \left(\frac{\alpha}{\beta}\right)^{\lceil \log_\beta x \rceil - \log_\beta x} x^{\log_\beta \alpha} \\ &= \Theta(x^{\log_\beta \alpha}) \,. \end{aligned}$$

□

Une généralisation de ce dernier résultat est le contenu du très fameux "Master Theorem", dont nous ne donnerons pas la preuve ici.

Théorème 2.24 ("Master Theorem"). *Soient $\alpha \geqslant 1$, $\beta > 1$ des constantes et $f : \mathbb{N} \to \mathbb{R}_+$ une fonction. Pour une suite $(a_N)_{N\in\mathbb{N}}$ solution de la récurrence diviser-pour-régner* (2.3) *:*

Cas 1. Si $f(N) = O(N^{\log_\beta \alpha - \varepsilon})$ pour $\varepsilon > 0$, alors $a_N = \Theta(N^{\log_\beta \alpha})$.

Cas 2. Si $f(N) = \Theta(N^{\log_\beta \alpha})$, alors $a_N = \Theta(N^{\log_\beta \alpha} \log_2 N)$.

Cas 3. Si $f(N) = \Omega(N^{\log_\beta \alpha + \varepsilon})$ pour $\varepsilon > 0$, et si $\alpha f(N/\beta) \leqslant C f(N)$ pour une certaine constante $C < 1$ et N suffisamment grand, alors $a_N = \Theta(f(N))$.

□

2.4 Application : produit matriciel selon Strassen

On s'intéresse au problème consistant à calculer le produit de deux matrices $n \times n$. (La taille du problème est donc n.) Considérons donc deux matrices de taille $n \times n$

$$A = (a_{ij})$$
$$B = (b_{ij})$$

où $i, j \in [n]$. Pour rappel, la matrice produit $C = AB$ s'obtient comme suit :

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \,. \tag{2.5}$$

Le coefficient c_{ij} situé sur la i-ème ligne et j-ème colonne de C est le produit scalaire de la i-ème ligne de A et j-ème colonne de B.

L'algorithme classique calcule les n^2 coefficients c_{ij} en utilisant directement (2.5). Pour chaque coefficent c_{ij}, cet algorithme effectue n multiplications et $n-1$ additions. Au total, l'algorithme effectue $n^2 \cdot n = n^3$ multiplications et $n^2 \cdot (n-1) = n^3 - n^2$ additions. Ce qui fait un total de $2n^3 - n^2 = \Theta(n^3)$ opérations arithmétiques. Cependant, il existe un algorithme qui fait (asymptotiquement) *mieux*, l'*algorithme de Strassen* (1969).

Pour $n = 2$, on a :

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

et l'algorithme classique calcule

$$\begin{aligned} c_{11} &= a_{11}b_{11} + a_{12}b_{21} \\ c_{12} &= a_{11}b_{12} + a_{12}b_{22} \\ c_{21} &= a_{21}b_{11} + a_{22}b_{21} \\ c_{22} &= a_{21}b_{12} + a_{22}b_{22} \,. \end{aligned}$$

Au total, 8 multiplications et 4 additions sont effectuées. L'algorithme de Strassen est basé sur le fait que pour $n = 2$, il est possible de calculer un produit matriciel en effectuant 7 *multiplications et* 18 *additions*.

Remarque 2.25. Pour $n = 2$, le nombre total d'opérations arithmétiques ne diminue pas, mais *augmente*. Cependant, nous verrons que le fait de pouvoir calculer le produit en seulement 7 multiplications va permettre, pour des valeurs de n plus grandes, de *diminuer* le nombre total d'opérations arithmétiques.

Strassen a observé qu'en calculant les 7 produits

$$\begin{aligned} I &= (a_{11} - a_{22}) \cdot (b_{21} + b_{22}) \\ II &= (a_{11} + a_{22}) \cdot (b_{11} + b_{22}) \\ III &= (a_{11} - a_{21}) \cdot (b_{11} + b_{12}) \\ IV &= (a_{11} + a_{12}) \cdot b_{22} \\ V &= a_{11} \cdot (b_{12} - b_{22}) \\ VI &= a_{22} \cdot (b_{21} - b_{11}) \\ VII &= (a_{21} + a_{22}) \cdot b_{11} \end{aligned}$$

la matrice $C = AB$ peut s'obtenir comme suit :

$$\begin{aligned} c_{11} &= I + II - IV + VI \\ c_{12} &= IV + V \\ c_{21} &= VI + VII \\ c_{22} &= II - III + V - VII \,. \end{aligned}$$

Exemple 2.26. Par exemple,

$$\begin{aligned} IV + V &= (a_{11} + a_{12}) \cdot b_{22} + a_{11} \cdot (b_{12} - b_{22}) \\ &= a_{11}b_{22} + a_{12}b_{22} + a_{11}b_{12} - a_{11}b_{22} \\ &= a_{11}b_{12} + a_{12}b_{22} \\ &= c_{12} \,. \end{aligned}$$

Observons que ce résultat n'utilise *pas* la commutativité du corps $\mathbb{R}_{+,\cdot}$. Les formules restent vraies dans tout anneau, et en particulier dans l'anneau des matrices $k \times k$ réelles, $M_{k\times k}(\mathbb{R})$.

Pour $n > 2$, l'algorithme de Strassen découpe chaque matrice en quatre sous-matrices $\frac{n}{2} \times \frac{n}{2}$ (si n est impair, les tailles sont $\lfloor n/2 \rfloor \times \lfloor n/2 \rfloor$, $\lfloor n/2 \rfloor \times \lceil n/2 \rceil$, $\lceil n/2 \rceil \times \lfloor n/2 \rfloor$ et $\lceil n/2 \rceil \times \lceil n/2 \rceil$) :

$$\left(\begin{array}{c|c} A_{11} & A_{12} \\ \hline A_{21} & A_{22} \end{array}\right) \left(\begin{array}{c|c} B_{11} & B_{12} \\ \hline B_{21} & B_{22} \end{array}\right) = \left(\begin{array}{c|c} C_{11} & C_{12} \\ \hline C_{21} & C_{22} \end{array}\right) \,.$$

De nouveau, on a (exercice) :

$$\begin{aligned} C_{11} &= A_{11}B_{11} + A_{12}B_{21} \\ C_{12} &= A_{11}B_{12} + A_{12}B_{22} \\ C_{21} &= A_{21}B_{11} + A_{22}B_{21} \\ C_{22} &= A_{21}B_{12} + A_{22}B_{22} \,. \end{aligned}$$

Donc les formules de Strassen s'appliquent, et on peut calculer C_{11}, C_{12}, C_{21}, C_{22} en effectuant 7 produits matriciels et 18 additions matricielles. L'algorithme de Strassen effectue les additions matricielles directement et les produits matriciels récursivement.

Soit $T(n)$ le nombre total d'opérations arithmétiques (multiplications et additions de nombres réels) pour calculer le produit de deux matrices $n \times n$. On trouve la récurrence diviser-pour-régner suivante :

$$T(n) = 7 \cdot T(n/2) + 18 \cdot n^2.$$

Pour trouver le comportement asymptotique de $T(n)$, on utilise le "Master Theorem" avec $\alpha = 7$, $\beta = 2$ et $f(n) = 18n^2$. On commence par le calcul $\log_\beta \alpha = 2,81\ldots > 2$. Par conséquent,

$$f(n) = O(n^2) = O(n^{\log_\beta \alpha - \varepsilon})$$

et on est donc dans le Cas 1 (prendre par exemple ε tel que $\log_\beta \alpha - \varepsilon = 2,81$). Par le "Master Theorem", on trouve

$$T(n) = \Theta(n^{\log_\beta \alpha}) = \Theta(n^{2,81\ldots}) .$$

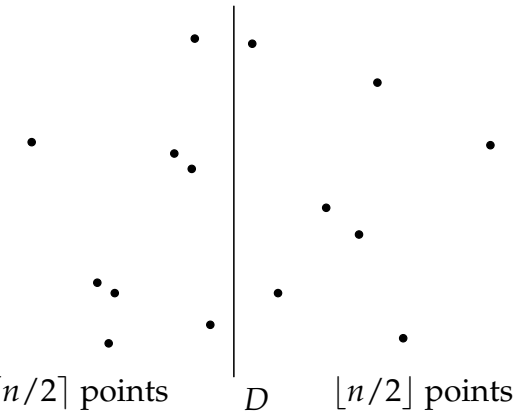
L'algorithme de Strassen est donc (asymptotiquement) meilleur que l'algorithme classique !

Remarque 2.27.
- Tout algorithme calculant le produit de deux matrices $n \times n$ est de complexité $\Omega(n^2)$, parce qu'il faut calculer n^2 coefficients.
- Coppersmith et Vinograd (1990) ont obtenu un algorithme calculant le produit de deux matrices $n \times n$ en $O(n^{2,376})$.
- Conjecture : pour tout $\varepsilon > 0$ il existe un algorithme en $O(n^{2+\varepsilon})$ (voir par exemple, Cohn, Kleinberg, Szegedy et Umans (2005)).
- On peut démontrer que les problèmes suivants sont de la même complexité que le calcul du produit de deux matrices $n \times n$:
  1. inversion d'une matrice $n \times n$;
  2. résolution d'un système $Ax = b$ de n équations linéaires à n variables ;
  3. calcul d'un déterminant $n \times n$.

2.5 Application : recherche d'une plus proche paire

Etant donné n points dans le plan (pour simplifier, nous supposerons que toute droite verticale ou horizontale contient $\leqslant 1$ de ces n points), comment trouver (rapidement) une paire de points séparés par une distance minimale ?

L'algorithme trivial consistant à considérer chaque paire de points est en $\Theta(n^2)$. On aimerait faire mieux. Notre point de départ est d'implémenter une stratégie diviser-pour-régner. En gros, nous voulons diviser le problème en deux sous-problèmes de taille $n/2$ (si n est impair, les tailles sont $\lfloor n/2 \rfloor$ et $\lceil n/2 \rceil$), récurser, et recombiner.



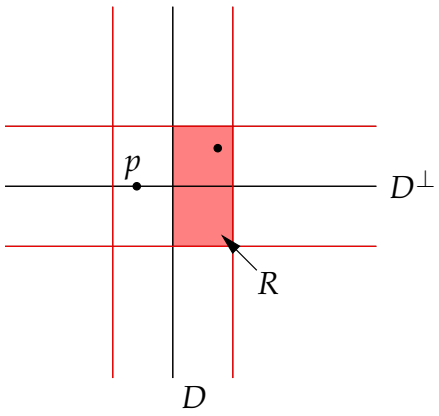
La figure ci-dessus illustre notre manière de diviser le problème : choisir une verticale D ne contenant aucun des n points et coupant le nuage de points en deux. Ceci semble être une bonne idée, mais comment recombiner ?

Soit d en distance minimum observée à gauche ou à droite lors des appels récursifs. Pour résoudre le problème original, nous devons voir s'il existe une paire p, q de points avec p

à gauche, q à droite et $d(p,q) < d$, et s'il existe un telle paire en trouver une avec $d(p,q)$ minimum.

Quelques observations :

1. On peut ignorer les points à distance $> d$ de la verticale D car tout point situé à une distance $> d$ de la droite D est situé à une distance $> d$ des points de l'autre côté de D.
2. On a $d(p,q) < d$ pour une paire p,q seulement si $d(p,D) \leqslant d$ et q se trouve dans un rectangle $2d \times d$ déterminé par p (voir dessin ci-dessous). Notons $D^\perp$ la perpendiculaire à D passant par p. Les seuls points q qui nous intéressent sont ceux tels que $d(q,D) \leqslant d$ et $d(q,D^\perp) \leqslant d$. L'ensemble de tous les points x tels que $d(x,D) \leqslant d$, $d(x,D^\perp) \leqslant d$ et x est situé à droite de D est un rectangle $2d \times d$ que nous noterons $R = R(p)$.



Combien de points q peut-on trouver dans le rectangle R ? Nous savons bien sûr que deux points q, q' dans le rectangle R figurant parmi les n points donnés en entrée vérifient $d(q,q') \geqslant d$. Il résulte de ceci que le nombre de points q figurant parmi les n points donnés et appartenant au rectangle R est borné. Intuitivement, on dirait que le maximum est 6. Vérifions qu'il y a au plus 10 tels points q.

Lemme 2.28. *Soient $d > 0$, R un rectangle $2d \times d$ et $X \subseteq R$ un ensemble de points tels que $d(q,q') \geqslant d$ pour tous $q, q' \in X$ distincts. Alors $|X| \leqslant 10$.*

Démonstration. Autour de chaque point $q \in X$, on considère une boule ouverte $B(q)$ de rayon $d/2$. Si deux de ces boules se rencontrent, alors les centres q et q' sont tels que $d(q,q') < d/2 + d/2 = d$, ce qui contredit $d(q,q') \geqslant d$. Donc les boules $D(q)$ avec $q \in X$ sont disjointes.

Chacune de ces boules a au moins $1/4$ de sa surface dans le rectangle R. Par conséquent,

$$|X| \cdot \frac{1}{4} \cdot \pi \frac{d^2}{4} \leqslant 2d^2$$

d'où on tire $|X| \leqslant 32/\pi = 10,18\ldots$, ce qui implique $|X| \leqslant 10$ vu que $|X|$ est entier. □

Voici un algorithme diviser-pour-régner pour le problème de la plus proche paire. Nous noterons $T(n)$ la complexité en temps de la partie récursive de l'algorithme pour une instance de taille n.

– **Précalcul**. Construire deux listes triées, l'une contenant l'ensemble des points triés par abscisses croissantes, et l'autre liste contenant l'ensemble des points triés par ordonnées croissantes. [$\Theta(n \lg n)$]
– **Partie récursive**.

1. Trouver une droite verticale D divisant l'ensemble des points en deux parties, de tailles $\lceil n/2 \rceil$ et $\lfloor n/2 \rfloor$. [$\Theta(n)$]
2. Déterminer récursivement une paire la plus proche dans chacune des parties (gauche et droite), soit d la distance minimum observée. [$T(\lceil n/2 \rceil) + T(\lfloor n/2 \rfloor)$]
3. Pour tous les points p à gauche de D *et* à distance $\leqslant d$ de D, inspecter tous les points q à droite de D, dans le rectangle $R(p)$ défini par p, retenir la distance minimum si celle-ci est $< d$, et une paire à distance minimum. [$\Theta(n)$]
4. Retourner la distance minimum et une paire de points à distance minimum. [$\Theta(1)$]

On trouve la récurrence diviser-pour-régner suivante :

$$T(n) = 2T(n/2) + \Theta(n),$$

qui a pour solution

$$T(n) = \Theta(n \log_2 n)\ .$$

A cela on rajoute $\Theta(n \log_2 n)$ pour le précalcul. Au total, le problème peut être résolu en $O(n \log_2 n)$. Ceci est mieux que l'algorithme trivial en $\Theta(n^2)$!

2.6 Autres types de récurrences

Les types de récurrences vus jusqu'ici sont principalement :
– les récurrences linéaires à coefficients constants,
– les récurrences diviser-pour-régner.
Nous terminons ce chapitre par deux exemples de récurrences d'autres types, chacun placé dans son contexte.

2.6.1 Calcul d'une racine carrée

Considérons la récurrence suivante :

$$a_n = \frac{1}{2}\left(a_{n-1} + \frac{\beta}{a_{n-1}}\right) \quad n \geq 1; \quad a_0 = 1\ . \tag{2.6}$$

C'est une récurrence non linéaire, d'ordre 1, utilisée pour calculer la racine carrée $\sqrt{\beta}$ d'un réel $\beta > 0$ par le biais de la méthode de Newton. Notre but est de démontrer que $(a_n)_{n\in\mathbb{N}}$ converge très rapidement vers $\sqrt{\beta}$.

Pour commencer, supposons que $\lim_{n\to\infty} a_n$ existe et est égale à L, avec $L \neq 0$. Alors on peut déterminer la valeur de L en utilisant la récurrence. En effet,

$$\underbrace{\lim_{n\to\infty} a_n}_{=L} = \underbrace{\lim_{n\to\infty} \frac{1}{2}\left(a_{n-1} + \frac{\beta}{a_{n-1}}\right)}_{} = \frac{1}{2}\underbrace{\lim_{n\to\infty} a_{n-1}}_{=L} + \frac{1}{2}\beta \underbrace{\frac{1}{\lim_{n\to\infty} a_{n-1}}}_{=1/L}$$

et donc

$$L = \frac{1}{2}L + \frac{1}{2}\frac{\beta}{L}\ .$$

En résolvant cette équation, on trouve $L = \pm\sqrt{\beta}$. Notons que $a_0 = 1$, ce qui implique $a_1 > 0$, puis $a_2 > 0$, etc... Donc on a $L = \sqrt{\beta}$.

Montrons maintenant que $(a_n)_{n\in\mathbb{N}}$ converge, vers un nombre différent de 0. L'argument heuristique du paragraphe précédent nous invite à poser $b_n := a_n - \sqrt{\beta}$ pour $n \in \mathbb{N}$, c'est-à-dire $a_n = b_n + \sqrt{\beta}$. Réécrivons la récurrence, mais cette fois-ci pour la suite $(b_n)_{n\mathbb{N}}$:

$$\begin{aligned} b_n + \sqrt{\beta} &= \frac{1}{2}\left(b_{n-1} + \sqrt{\beta} + \frac{\beta}{b_{n-1}+\sqrt{\beta}}\right) \\ \iff b_n &= \frac{1}{2}\left(b_{n-1} - \sqrt{\beta} + \frac{\beta}{b_{n-1}+\sqrt{\beta}}\right) \\ \iff b_n &= \frac{1}{2}\left(\frac{b_{n-1}^2 - (\sqrt{\beta})^2 + \beta}{b_{n-1}+\sqrt{\beta}}\right) = \frac{1}{2}\frac{b_{n-1}^2}{b_{n-1}+\sqrt{\beta}} \end{aligned}$$

(ci-dessus nous avons pris $n \geqslant 1$, évidemment). De plus, $b_0 = a_0 - \sqrt{\beta} = 1 - \sqrt{\beta}$. Notons que cette dernière quantité est négative quand $\beta > 1$. Ce n'est pas un problème car $b_1 = \frac{1}{2}\frac{(1-\sqrt{\beta})^2}{1+\sqrt{\beta}} \geqslant 0$, ce qui implique $b_2 \geqslant 0$, etc...

Théorème 2.29. *Pour tout $\beta > 0$, la solution $(a_n)_{n\in\mathbb{N}}$ de la récurrence* (2.6) *converge vers $\sqrt{\beta}$.*

Démonstration. Par ce qui précède, il suffit de démontrer que b_n tend vers 0 pour $n \to \infty$. On aura alors

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty}(b_n + \sqrt{\beta}) = 0 + \sqrt{\beta}\,.$$

Pour $n \geqslant 2$, nous avons $b_n \geqslant 0$ et $b_{n-1} \geqslant 0$ et donc :

$$0 \leqslant b_n = \frac{1}{2}\frac{b_{n-1}^2}{b_{n-1}+\sqrt{\beta}} \leqslant \frac{1}{2}\frac{b_{n-1}^2}{b_{n-1}} \leqslant \frac{1}{2}b_{n-1}$$

Donc $(b_n)_{n\in\mathbb{N}}$ converge vers 0 (voyez-vous pourquoi ?). □

Remarque 2.30. On sait déjà que $b_n \overset{n\to\infty}{\longrightarrow} 0$ et donc $a_n \overset{n\to\infty}{\longrightarrow} \sqrt{\beta}$. Dès que b_{n-1} est petit, disons $b_{n-1} \ll \sqrt{\beta}$, on a :

$$b_n \approx \frac{1}{2\sqrt{\beta}} b_{n-1}^2$$

ce qui implique que le nombre de chiffres de $\sqrt{\beta}$ qui sont corrects dans a_n *double* (essentiellement) à chaque itération.

Exemple 2.31. Pour $\beta = 2$, on trouve les valeurs suivantes.

n	a_n	$b_n = a_n - \sqrt{2}$
1	$1,5$	$0,0857\ldots < 10^{-1}$
2	$1,\underline{41}666\ldots$	$0,00245\ldots < 10^{-2}$
3	$1,\underline{4142}1568\ldots$	$0,000002123\ldots < 10^{-4}$
4	$1,\underline{4142135623}\ldots$	$\approx 2\cdot 10^{-12} < 10^{-8}$
5	$1,\underline{414213562373}\ldots$	$< 10^{-16}$

2.6.2 Fractions continuées

Comme dernier exemple, étudions la récurrence non linéaire d'ordre 1 suivante :

$$a_n = \frac{1}{1+a_{n-1}} \quad \forall n \geqslant 1; \quad a_0 = 1\,.$$

Pour $n \leqslant 4$:

$$\begin{aligned}
a_0 &= 1 = \frac{1}{1} \\
a_1 &= \frac{1}{1+1} = \frac{1}{2} \\
a_2 &= \frac{1}{1+\dfrac{1}{1+1}} = \frac{2}{3} \\
a_3 &= \frac{1}{1+\dfrac{1}{1+\dfrac{1}{1+1}}} = \frac{3}{5} \\
a_4 &= \frac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+1}}}} = \frac{5}{8}\,.
\end{aligned}$$

Aha ! On dirait que les valeurs obtenues sont des quotients de nombres de Fibonacci consécutifs. Vérifions cela en posant, pour $n \geqslant 1$:

$$a_n = \frac{b_{n-1}}{b_n}\,.$$

Pour $n \geqslant 2$, on obtient alors :

$$\begin{aligned}
&\frac{b_{n-1}}{b_n} = \frac{1}{1+\frac{b_{n-2}}{b_{n-1}}} \\
\iff &\frac{b_{n-1}}{b_n} = \frac{b_{n-1}}{b_{n-1}+b_{n-2}} \\
\iff &b_n = b_{n-1} + b_{n-2}
\end{aligned}$$

Donc $(b_n)_{n\in\mathbb{N}}$ satisfait la même récurrence que les nombres de Fibonacci, mais avec des conditions initiales différentes :

$$a_1 = \frac{b_0}{b_1} = \frac{1}{2} \Longrightarrow b_0 = 1,\ b_1 = 2\,.$$

On trouve donc $b_n = F_{n+2}$ pour $n \in \mathbb{N}$.

La limite $\lim_{n\to\infty} a_n$ est amusante à calculer :

$$\lim_{n\to\infty} a_n = \frac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\dfrac{1}{1+\cdots}}}}\,.$$

On appelle ce type de fraction une *fraction continuée*. De telles expressions se révèlent utiles pour approximer des nombres (ir)rationnels par des rationnels dont la *taille*, c'est-à-dire le nombre de bits total dans la représentation du rationnel en base 2, est petite.

Etant donné que $a_n = \frac{F_{n+1}}{F_{n+2}}$ et que $F_n \sim \frac{1}{\sqrt{5}}\varphi^n$, on a

$$\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\cdots}}}} = \lim_{n\to\infty} \frac{\frac{1}{\sqrt{5}}\varphi^{n+1}}{\frac{1}{\sqrt{5}}\varphi^{n+2}} = \frac{1}{\varphi} = 0,618\ldots$$

2.7 Exercices

Exercice 2.1. De combien de façons différentes peut-on monter un escalier de 30 marches, si on monte à chaque pas soit d'une seule marche soit de deux marches à la fois ?

Exercice 2.2. Que vaut le déterminant de la matrice $n \times n$

$$\begin{pmatrix} 1 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 1 & -1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 1 & -1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 1 \end{pmatrix} \quad ?$$

Exercice 2.3. Que vaut

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} \quad ?$$

Exercice 2.4. Prouver que, pour tout entier $n \geqslant 1$,

$$\varphi^n = F_n \cdot \varphi + F_{n-1}\ ,$$

où $\varphi := \frac{1+\sqrt{5}}{2}$ est le *nombre d'or*.

Exercice 2.5. Prouver que, pour tout entier $n \geqslant 3$,

$$F_n > \varphi^{n-2}$$

Exercice 2.6. Résoudre les récurrences

(i) $a_n = \frac{1}{2}a_{n-1} + 1$ pour $n \geqslant 1$, $\quad a_0 = 1$

(ii) $a_n = 5a_{n-1} - 6a_{n-2}$ pour $n \geqslant 2$, $\quad a_0 = -1, \quad a_1 = 1$

(iii) $a_n = 6a_{n-1} - 9a_{n-2}$ pour $n \geqslant 2$, $\quad a_0 = 1, \quad a_1 = 9$

(iv) $a_n = 4a_{n-1} - 3a_{n-2} + 2^n$ pour $n \geqslant 2$, $\quad a_0 = 1, \quad a_1 = 11$

Exercice 2.7. Résoudre les récurrences

(i) $a_{n+2} = 3a_{n+1} + 4a_n$ pour $n \geqslant 0$, $\quad a_0 = 1, \quad a_1 = 3$

(ii) $a_{n+3} - 6a_{n+2} + 11a_{n+1} - 6a_n$ pour $n \geqslant 0$, $\quad a_0 = 2, \quad a_1 = 0, \quad a_2 = -2$

(iii) $a_{n+3} = 3a_{n+1} - 2a_n$ pour $n \geqslant 0$, $\quad a_0 = 1, \quad a_1 = 0, \quad a_2 = 0$

(iv) $a_{n+3} + 3a_{n+2} + 3a_{n+1} + a_n = 0$

(v) $a_{n+4} + 4a_n = 0$

Exercice 2.8. Résoudre la récurrence

$$\begin{aligned} &a_{n+2} - (2\cos\alpha)a_{n+1} + a_n = 0 \quad \forall n \geqslant 0 \\ &a_1 = \cos\alpha, \quad a_2 = \cos 2\alpha \end{aligned}$$

Exercice 2.9. Résoudre les récurrences

(i) $a_n + 2a_{n-1} = n + 3$ pour $n \geqslant 1$ $\qquad a_0 = 3$

(ii) $a_{n+2} + 8a_{n+1} - 9a_n = 8 \cdot 3^{n+1}$ pour $n \geqslant 0$ $\qquad a_0 = 2, \quad a_1 = -6$

(iii) $a_{n+2} - 6a_{n+1} + 9a_n = 2^n + n$ pour $n \geqslant 0$

(iv) $na_n = (n+3)a_{n-1} + n^2 + n$ pour $n \geqslant 1$

Exercice 2.10. Que vaut le déterminant de la matrice $n \times n$

$$\begin{pmatrix} 2 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 1 & 2 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 2 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 2 \end{pmatrix} \quad ?$$

Exercice 2.11. Avec l'alphabet $\{A, B, C\}$, combien peut-on écrire de mots de n lettres dans lesquels on ne trouve pas

(i) deux lettres A côte-à-côte ?

(ii) deux lettres A ni deux lettres B côte-à-côte ?

(iii) deux lettres A ni deux lettres B ni deux lettres C côte-à-côte ?

Exercice 2.12. Donner le comportement asymptotique des suites $T(n)$ pour chacune des récurrences suivantes :

(i) $T(n) = 2T(\lceil n/2 \rceil) + n^2$

(ii) $T(n) = T(\lfloor 9n/10 \rfloor) + n$

(iii) $T(n) = 16T(\lceil n/4 \rceil) + n^2$

(iv) $T(n) = 7T(\lceil n/3 \rceil) + n^2$

(v) $T(n) = 7T(\lceil n/2 \rceil) + n^2$

(vi) $T(n) = 2T(\lfloor n/4 \rfloor) + \sqrt{n}$

(vii) $T(n) = T(n-1) + n$

(viii) $T(n) = T(\lfloor \sqrt{n} \rfloor) + 1$

Exercice 2.13. Résoudre la récurrence

$$\begin{aligned} &a_n = \sqrt{a_{n-1}a_{n-2}} \quad \forall n \geqslant 2 \\ &a_0 = 1, \quad a_1 = 2 \end{aligned}$$

Exercice 2.14. (Examen août 2011.) Combien y a-t-il de matrices $2 \times n$ à coefficients entiers vérifiant les deux conditions suivantes ?

– Dans chacune des deux lignes, chacun des entiers $1, 2, \ldots, n$ apparaît une et une seule fois.

– Dans chacune des n colonnes, les deux coefficients diffèrent d'au plus 1.

Exercice 2.15. (Examen août 2011.) Soient x et y deux naturels de $2n$ bits, c'est-à-dire dont l'écriture binaire occupe au plus $2n$ bits. Soient X_0, X_1, Y_0 et Y_1 quatre naturels de n bits tels que $x = 2^n X_1 + X_0$ et $y = 2^n Y_1 + Y_0$.

a) Vérifier que

$$xy = (2^{2n} + 2^n)X_1Y_1 + 2^n(X_1 - X_0)(Y_0 - Y_1) + (2^n + 1)X_0Y_0 \,.$$

b) Considérons l'algorithme récursif qui multiplie les naturels x et y en appliquant l'équation ci-dessus. Soit $f(n)$ le nombre d'opérations simples (additions ou soustractions de bits, décalages, comparaisons… etc) nécessaires pour le calcul récursif du produit xy par le biais de cette équation. Ecrire une relation de récurrence du type "diviser pour régner" pour $f(n)$. (Il n'est pas nécessaire de calculer avec précision le nombre d'opérations simples requises, calculer ce nombre à une constante près est suffisant.)

c) Sur base de cette récurrence, déterminer le comportement asymptotique de $f(n)$.

Exercice 2.16. (Difficile.) Résoudre la récurrence (discuter en fonction de a_0)

$$a_n = a_{n-1}^2 + 2 \quad \forall n \geqslant 1$$

(Hint : poser $a_n = b_n + 1/b_n$.)

Exercice 2.17. (Difficile.) Montrer que la solution de la récurrence

$$\begin{aligned} a_n &= \sin(a_{n-1}) \quad \forall n \geqslant 1 \\ a_0 &= 1 \end{aligned}$$

vérifie $\lim_{n\to\infty} a_n = 0$ et $a_n = O(1/\sqrt{n})$. (Hint : poser $b_n = 1/a_n$.)

Chapitre 3

Fonctions génératrices

"Une fonction génératrice est une corde à linge où on peut pendre les termes d'une suite."

3.1 Exemples

3.1.1 Les nombres de Catalan

Quel est le nombre de manières c_n de parenthéser un produit de n facteurs $x_1, \ldots, x_n$ (on cherche un parenthésage complet) ? Ce nombre c_n s'appelle n-ème *nombre de Catalan*.

Exemple 3.1. Pour $n = 1$ et $n = 2$, on trouve les parenthésages triviaux

$$x_1 \quad \text{et} \quad x_1 x_2 \,.$$

Pour $n = 3$, il y a 2 parenthésages :

$$(x_1 x_2)x_3 \quad \text{et} \quad x_1(x_2 x_3) \,.$$

Pour $n = 4$, il y a 5 parenthésages :

$$((x_1 x_2)x_3)x_4 \,, \quad (x_1(x_2 x_3))x_4 \,, \quad (x_1 x_2)(x_3 x_4) \,, \quad x_1((x_2 x_3)x_4) \,, \quad \text{et} \quad x_1(x_2(x_3 x_4)) \,.$$

Jusqu'ici, on a obtenu $c_1 = 1$, $c_2 = 1$, $c_3 = 2$ et $c_4 = 5$. Par convention, nous poserons $c_0 := 0$.

Une motivation pour chercher la valeur du n-ème nombre de Catalan c_n est par exemple le problème suivant : comment parenthéser un produit de n matrices (de tailles potentiellement différentes) pour minimiser le nombre de multiplications nécessaires pour évaluer le produit, avec un algorithme donné ?

Supposons qu'on utilise l'algorithme classique pour évaluer le produit. Une première chose à noter est que le nombre de multiplications de nombres réels dépend effectivement du parenthésage !

Exemple 3.2. Considérons un produit de $n = 4$ matrices M_1, M_2, M_3 et M_4 de tailles respectives 5×2, 2×3, 3×7 et 7×2. Le produit est de taille 5×2. Le parenthésage $M_1((M_2 M_3)M_4)$ requiert $14 \cdot 3 + 4 \cdot 7 + 10 \cdot 2 = 90$ multiplications, tandis que le parenthésage $(M_1 M_2)(M_3 M_4)$ requiert $15 \cdot 2 + 6 \cdot 7 + 10 \cdot 3 = 102$ multiplications.

Il n'est pas immédiatement clair comment résoudre le problème de manière efficace. Quid de la solution consistant à essayer toutes les possibilités ? Comme il y a c_n parenthésages, l'algorithme sera de complexité $\Omega(c_n)$.

En réfléchissant bien, on peut obtenir un algorithme de complexité $O(n^3)$ pour calculer le meilleur parenthésage, basé sur la programmation dynamique (ceci est un bon exercice). On verra plus loin que $c_n = \Omega((4-\varepsilon)^n)$ pour tout $\varepsilon > 0$. Donc c_n est "en gros" une exponentielle de base 4, qui grandit beaucoup plus vite qu'un polynôme de degré 3. On s'y attendait, mais on a ici la confirmation que la solution consistant à considérer toutes les possibilités est à proscrire.

On peut obtenir une équation de récurrence pour c_n, en se basant sur l'observation suivante : le dernier produit effectué (cas où il y a n facteurs) est constitué du produit des k premiers facteurs (déjà multipliés entre eux) et du produit des $n-k$ derniers facteurs (déjà multipliés entre eux), où $k = 1, \ldots, n-1$. Donc,

$$c_n = \sum_{k=1}^{n-1} c_k c_{n-k} = c_1 c_{n-1} + c_2 c_{n-2} + \cdots + c_{n-1} c_1 \quad \forall n \geqslant 2; \quad c_1 = 1 \tag{3.1}$$

Théorème 3.3. *Pour tout $n \geqslant 1$, le n-ème nombre de Catalan est*

$$c_n = \frac{1}{n}\binom{2n-2}{n-1}.$$

Démonstration. Considérons la *fonction génératrice ordinaire* $C(x)$ des nombres de Catalan c_n, c'est-à-dire la fonction

$$C(x) := \sum_{n=1}^{\infty} c_n x^n,$$

sans s'occuper de convergence (pour le moment). Alors

$$\begin{aligned} C(x) &= c_1 x + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n + \cdots \\ &= x + (c_1 c_1)x + (c_1 c_2 + c_2 c_1)x^3 + \cdots (c_1 c_{n-1} + \cdots + c_{n-1} c_1)x^n + \cdots \\ &= x + \left(c_1 x + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n + \cdots\right)\left(c_1 x + c_2 x^2 + c_3 x^3 + \cdots + c_n x^n + \cdots\right). \end{aligned}$$

Ces égalités sont justifiées du point de vue des séries formelles : quand on compare, pour un $n \in \mathbb{N}$ donné, le coefficient de x^n dans les deux membres, on a égalité. Nous obtenons l'équation fonctionnelle :

$$C(x) = x + [C(x)]^2 \ . \tag{3.2}$$

Résolvons cette équation du second degré :

$$[C(x)]^2 - [C(x)] + x = 0 \iff C(x) = \frac{1 \pm \sqrt{1-4x}}{2}.$$

On trouve deux fonctions solution :

$$\frac{1}{2} + \frac{1}{2}\sqrt{1-4x} \quad \text{et} \quad \frac{1}{2} - \frac{1}{2}\sqrt{1-4x}\,.$$

Une de ces solutions peut être éliminée. En effet, on a $C(0) = 0$ car la série définissant $C(x)$ n'a pas de terme indépendant (qui plus est, on a posé $c_0 := 0$). Donc,

$$C(x) = \frac{1}{2} - \frac{1}{2}\sqrt{1-4x}\,.$$

Par la formule de la série du binôme de Newton,

$$\begin{aligned} C(x) &= \frac{1}{2} - \frac{1}{2}\sum_{n=0}^{\infty} \binom{1/2}{n} (-4x)^n \\ &= -\frac{1}{2}\sum_{n=1}^{\infty} (-1)^n \binom{1/2}{n} 4^n x^n, \end{aligned}$$

où $\binom{1/2}{0} := 1$ par convention, et

$$\binom{1/2}{n} = \frac{\frac{1}{2}(\frac{1}{2}-1)\dots(\frac{1}{2}-n+1)}{n!}$$

pour $n \geqslant 1$. On trouve

$$\begin{aligned} c_n &= (-1)^{n+1}\,\frac{1}{2}\cdot\frac{\overbrace{\frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)}^{n \text{ facteurs}}}{n!}\,2^{2n} \\ &= (-1)^{n+1}\,\frac{1}{2}\cdot\frac{1(1-2)\cdots(1-2n+2)}{n!}\,2^n \\ &= \frac{1}{2}\cdot\frac{1\cdot 1\cdot 3\cdot 5\cdots(2n-3)}{n!}\,2^n \\ &= \frac{1}{2}\cdot\frac{1\cdot 1\cdot 3\cdot 5\cdots(2n-3)}{n!\,n!}\,\underbrace{n!\,2^n}_{=2\cdot 4\cdot 6\cdots 2n} \\ &= \frac{1}{2}\cdot\frac{(2n-2)!}{n!\,n!}\,2n \\ &= \frac{1}{n}\cdot\frac{(2n-2)!}{(n-1)!\,(n-1)!} \\ &= \frac{1}{n}\binom{2n-2}{n-1}. \end{aligned}$$

□

Voyons maintenant les premières valeurs de c_n et comparons-les aux premières valeurs de F_n.

n	1	2	3	4	5	6	7	8	9	…
c_n	1	1	2	5	14	42	132	429	1430	…
F_n	1	1	2	3	5	8	13	21	34	…

On observe que $c_n \gg F_n$. Les deux suites ont un comportement exponentiel, mais de base différente. On verra plus tard $c_n = \Omega((4-\varepsilon)^n)$ (pour tout $\varepsilon > 0$) et $F_n = \Theta(\varphi^n) = \Theta((\frac{1+\sqrt{5}}{2})^n = O((1.6181)^n)$.

Remarquons que pour tout $n \geqslant 2$ fixé, il existe une bijection entre :

(i) les parenthésages complets d'un produit de n facteurs, et

(ii) les arbres binaires enracinés à n feuilles (comptés à isomorphisme près).

On obtient le corollaire suivant (rappelons qu'il existe une bijection entre les arbres binaires enracinés et les triangulations d'un $(n+1)$-gone, voir Théorème 1.24).

Proposition 3.4. *Pour tout $n \geqslant 2$,*

$$\begin{aligned} \#(\textit{arbres binaires enracinés à n feuilles}) &= \#(\textit{triangulations d'un } (n+1)\textit{-gone}) \\ &= \textit{n-ème nombre de Catalan} \\ &= \frac{1}{n}\binom{2n-2}{n-1}. \end{aligned}$$

3.1.2 Retour sur les nombres de Fibonacci

Pour rappel, la suite de Fibonacci est définie par la RLCC suivante :

$$F_n = F_{n-1} + F_{n-2} \quad \forall n \geqslant 2; \quad F_0 = 0;\ F_1 = 1\,.$$

Posons maintenant

$$f(x) := \sum_{n=0}^{\infty} F_n x^n\,.$$

Alors on a :

$$\begin{aligned} f(x) &= \underbrace{0 + x}_{\text{conditions initiales}} + \sum_{n=2}^{\infty} F_n x^n \\ &= x + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) x^n \\ &= x + \sum_{n=2}^{\infty} F_{n-1} x^n + \sum_{n-2}^{\infty} F_{n-2} x^n \\ &= x + \underbrace{x \sum_{n=2}^{\infty} F_{n-1} x^{n-1}}_{=xf(x)} + \underbrace{x^2 \sum_{n=2}^{\infty} F_{n-2} x^{n-2}}_{=x^2 f(x)}\,. \end{aligned}$$

Comme pour les nombres de Catalan, on débouche sur une équation fonctionnelle :

$$(1 - x - x^2) f(x) = x\,.$$

En résolvant, on trouve

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

Décomposons maintenant $f(x)$ en fractions simples :

$$f(x) = \frac{\frac{1}{\sqrt{5}}}{1 - \varphi x} + \frac{\frac{-1}{\sqrt{5}}}{1 - \bar{\varphi} x}\,.$$

En utilisant l'identité :

$$\sum_{n=0}^{\infty} (\lambda x)^n = \frac{1}{1-\lambda x} ,$$

on obtient

$$\sum_{n=0}^{\infty} F_n x^n = f(x) = \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \varphi^n x^n - \frac{1}{\sqrt{5}} \sum_{n=0}^{\infty} \bar{\varphi}^n x^n .$$

Finalement, en identifiant le coefficient de x^n dans l'expression de gauche avec le coefficient de x^n dans l'expression de droite, on retombe sur la *formule de Binet* :

$$F_n = \frac{1}{\sqrt{5}} (\varphi^n - \bar{\varphi}^n) .$$

3.2 Fonctions génératrices ordinaires : théorie de base

Définition 3.5 (Fonction génératrice ordinaire)**.** La *fonction génératrice ordinaire* (FGO) de la suite

$$(a_n)_{n \in \mathbb{N}} = (a_0, a_1, a_2, \ldots)$$

est définie par

$$A(x) := \sum_{n=0}^{\infty} a_n x^n .$$

On note $[x^n]A(x)$ le coefficient de x^n dans $A(x)$, c'est-à-dire

$$[x^n]A(x) = a_n .$$

Remarque 3.6. La série définissant la FGO $A(x)$
- converge pour certains $x \in \mathbb{R}$;
- diverge pour d'autres $x \in \mathbb{R}$.

Pour le moment, on ignore les questions de convergence.
- Les manipulations effectuées sur les FGO sont bien définies si on les considère comme *séries formelles* ;
- Les séries auxquelles on s'intéresse ont typiquement de bonnes propriétés de convergence. En particulier, elles convergent la plupart du temps au moins pour

  $$x \in]-r; r[$$

  pour un certain choix de $r > 0$.

Exemple 3.7. La FGO de $(1, 1, 1, \ldots)$ est

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x} .$$

De manière plus générale, la FGO de $(1, \lambda, \lambda^2, \ldots, \lambda^n, \ldots)$ est

$$\frac{1}{1-\lambda x} .$$

Le résultat suivant va nous permettre d'obtenir la FGO d'une suite obtenue en faisant une opération simple (addition, multiplication, etc…) sur une ou plusieurs suite(s) dont on connaît la (les) FGO(s).

Théorème 3.8. *Soient $A(x)$ la FGO de $(a_n)_{n\in\mathbb{N}}$ et $B(x)$ la FGO de $(b_n)_{n\in\mathbb{N}}$. Alors :*

(i) $A(x)+B(x)$ *est la FGO de* $(a_n+b_n)_{n\in\mathbb{N}}$.

(ii) $xA(x)$ *est la FGO de* $(0,a_0,a_1,a_2,\ldots,a_{n-1},\ldots)$.

(iii) $\int_0^x A(t)\mathrm{d}t$ *est la FGO de* $(0,a_0,\frac{a_1}{2},\frac{a_2}{3},\ldots,\frac{a_{n-1}}{n},\ldots)$.

(iv) $\frac{A(x)-a_0}{x}$ *est la FGO de* $(a_1,a_2,a_3,\ldots,a_{n+1},\ldots)$.

(v) $A'(x)$ *est la FGO de* $(a_1,2a_2,3a_3,\ldots,(n+1)a_{n+1},\ldots)$.

(vi) $A(x)B(x)$ *est la FGO de* $(a_0,a_0b_1+a_1b_0,a_0b_2+a_1b_1+a_2b_0,\ldots)$.

(vii) $(1-x)A(x)$ *est la FGO de* $(a_0,a_1-a_0,a_2-a_1,\ldots,a_n-a_{n-1},\ldots)$.

(viii) $\frac{A(x)}{1-x}$ *est la FGO de* $(a_0,a_0+a_1,a_0+a_1+a_2,\ldots,\sum_{k=0}^n a_k,\ldots)$.

Démonstration. (i) (exercice facile).

(ii)
$$xA(x)=x\sum_{n=0}^{\infty}a_nx^n=\sum_{n=0}^{\infty}a_nx^{n+1}=0+\sum_{n=1}^{\infty}a_{n-1}x^n\,.$$

(iii)
$$\int_0^x A(t)\mathrm{d}t=\int_0^x\left(\sum_{n=0}^{\infty}a_nt^n\right)\mathrm{d}t=\sum_{n=0}^{\infty}\left(\int_0^x a_nt^n\mathrm{d}t\right)=\sum_{n=0}^{\infty}a_n\frac{x^{n+1}}{n+1}=\sum_{n=1}^{\infty}a_{n-1}\frac{x^n}{n}\,.$$

(iv) On a
$$A(x)-a_0=\sum_{n=1}^{\infty}a_nx^n=x\sum_{n=0}^{\infty}a_{n+1}x^n\,.$$
Il suffit alors de diviser par x.

(v)
$$A'(x)=\left(\sum_{n=0}^{\infty}a_nx^n\right)'=\sum_{n=1}^{\infty}a_nnx^{n-1}=\sum_{n=0}^{\infty}(n+1)a_{n+1}x^n\,.$$

(vi)
$$\begin{aligned}A(x)B(x)&=(a_0+a_1x+a_2x^2+\ldots)(b_0+b_1x+b_2x^2+\ldots)\\&=a_0b_0+(a_0b_1+a_1b_0)x+(a_0b_2+a_1b_1+a_2b_0)x^2+\ldots\\&=\sum_{n=0}^{\infty}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)x^n\,.\end{aligned}$$

(vii) Par (vi) : Si $B(x)$ est la FGO de $(1,-1,0,0,\ldots)$, alors $(1-x)A(x)=A(x)(1-x)=A(x)B(x)$ est la FGO de
$$(a_0,\underbrace{a_0(-1)+a_1(1)}_{=a_1-a_0},\ldots,\underbrace{a_0b_n+a_1b_{n-1}+\ldots}_{=0}+\underbrace{a_{n-1}(-1)+a_n(1)}_{=a_n-a_{n-1}},\ldots)\,.$$

(viii) Par (vi), de manière similaire, si $B(x)$ est la FGO de $(1,1,1,\ldots)$, alors $\frac{1}{1-x}A(x) = A(x)\frac{1}{1-x} = A(x)B(x)$ est la FGO de

$$(a_0, a_0+a_1, a_0+a_1+a_2, \ldots, \sum_{k=0}^{n} a_k, \ldots)\,.$$

□

Voyons quelques applications du théorème. Pour commencer, quelle est la FGO de la suite $(0,1,2,3,\ldots,n,\ldots)$?

$$\begin{array}{rrcl} & \dfrac{1}{1-x} & = & \text{FGO de } (1,1,1,1,\ldots) \\ \overset{(viii)}{\Longrightarrow} & \dfrac{1}{1-x}\cdot\dfrac{1}{1-x} & = & \text{FGO de } (1,1+1,1+1+1,\ldots) = (1,2,3,\ldots,n+1,\ldots) \\ \overset{(ii)}{\Longrightarrow} & \dfrac{x}{(1-x)^2} & = & \text{FGO de } (0,1,2,3,\ldots,n,\ldots)\,. \end{array}$$

En généralisant, on obtient le résultat suivant.

Proposition 3.9. *Pour $k \in \mathbb{N}$ fixé, la FGO de $\left(\binom{n}{k}\right)_{n\in\mathbb{N}}$ pour $k \in \mathbb{N}$ fixé est égal à*

$$\frac{x^k}{(1-x)^{k+1}}$$

Démonstration. En effet, c'est vrai pour $k = 0$. Vérifions que si c'est vrai pour k, alors ça l'est aussi pour $k+1$. Supposons donc que $\frac{x^k}{(1-x)^{k+1}}$ est la FGO de $\left(\binom{n}{k}\right)_{n\in\mathbb{N}}$. Alors, $\frac{x}{1-x}\cdot\frac{x^k}{(1-x)^{k+1}}$ est la FGO de

$$\begin{aligned} & \left(0, \binom{0}{k}, \binom{0}{k}+\binom{1}{k}, \binom{0}{k}+\binom{1}{k}+\binom{2}{k}, \ldots\right) \\ = & \left(\binom{0}{k+1}, \binom{1}{k+1}, \binom{2}{k+1}, \binom{3}{k+1}, \ldots\right) \\ = & \left(\binom{n}{k+1}\right)_{n\in\mathbb{N}}\,. \end{aligned}$$

Ci-dessus, on a utilisé l'identité de somme parallèle pour montrer la première égalité. □

Cherchons maintenant la FGO de $(0, 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots, \frac{1}{n}, \ldots)$. Par (iii), c'est

$$\int_0^x \frac{1}{1-t}\mathrm{d}t = \Big[-\ln(1-t)\Big]_0^x = \Big[\ln\frac{1}{1-t}\Big]_0^x = \ln\frac{1}{1-x} - 0\,.$$

Par (viii), la FGO de $\left(0, 1, 1+\frac{1}{2}, 1+\frac{1}{2}+\frac{1}{3}, \ldots, 1+\frac{1}{2}+\ldots+\frac{1}{n}, \ldots\right)$ est donc

$$\frac{1}{1-x}\ln\frac{1}{1-x}$$

Définition 3.10 (Nombre harmonique)**.** Pour $n \in \mathbb{N}$,

$$H_n := 1 + \frac{1}{2} + \ldots + \frac{1}{n}$$

est le n-ème *nombre harmonique*. (Pour $n = 0$, on a $H_0 := 0$.)

Proposition 3.11. *La FGO de la suite $(H_n)_{n\in\mathbb{N}}$ des nombres harmoniques est*

$$\frac{1}{1-x} \ln \frac{1}{1-x} .$$

Remarque 3.12. Pour tout choix de *noyau* $N(x, n)$, on peut définir une fonction génératrice via la série

$$\sum_{n=0}^{\infty} a_n \cdot N(x, n) .$$

Si on prend $N(x, n) = x^n$ on obtient les FGO et si on prend $N(x, n) = \frac{x^n}{n!}$ on obtient les FGE (fonctions génératrices exponentielles, voir plus loin).

3.3 Fonctions génératrices ordinaires : récurrences linéaires

On peut résoudre des RLCC (récurrences linéaires à coefficients constants) homogènes ou non homogènes en utilisant les FGO. Nous avons vu plus haut l'exemple des nombres de Fibonacci, dont la FGO est

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

Voyons un autre exemple facile, mais avec une RLCC non homogène cette fois.

Exemple 3.13. Soit $A(x)$ la FGO de la suite $(a_n)_{n\in\mathbb{N}}$ définie par :

$$a_n = 2a_{n-1} + 1 \quad \forall n \geq 1; \quad a_0 = 0 .$$

Alors

$$\begin{aligned} A(x) &= 0 + \sum_{n=1}^{\infty} (2a_{n-1} + 1)x^n \\ &= 0 + 2xA(x) + \underbrace{\left(\frac{1}{1-x} - 1\right)}_{=\frac{x}{1-x}} . \end{aligned}$$

Par conséquent,

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

En décomposant en fractions simples, on trouve

$$A(x) = \frac{1}{1-2x} - \frac{1}{1-x} = \sum_{n=0}^{\infty} 2^n x^n - \sum_{n=0}^{\infty} x^n = \sum_{n=0}^{\infty} (2^n - 1)x^n .$$

Donc

$$a_n = [x^n]A(x) = 2^n - 1 \quad \forall n \geq 0.$$

Ceci se généralise à toutes les RLCC. La méthode de résolution est la suivante :

(i) Déterminer la FGO $A(x)$ de la suite inconnue $(a_n)_{n\in\mathbb{N}}$. Celle-ci sera toujours une fonction rationnelle du type $A(x) = \frac{P(x)}{Q(x)}$ où P et Q sont des polynômes, et $\deg P < \deg Q$.

(ii) Décomposer $\frac{P(x)}{Q(x)}$ en fractions simples.

(iii) Extraire les coefficients en utilisant la décomposition.

3.4 Fonctions génératrices ordinaires : applications

3.4.1 Nombre moyen de comparaisons de Quicksort

Nous allons analyser l'algorithme *Quicksort* (Hoare, 1962) :

```
def partition(a, l, r, i):
  v := a[i]
  swap a[i] and a[r]
  s := l
  for k from l to r-1:
    if a[k] <= v:
      swap a[k] and a[s]
      s := s + 1
  swap a[s] and a[r]
  return s

def quicksort(a, l, r):
  if r > l:
    select a pivot index i
    new_i := partition(a, l, r, i)
    quicksort(a, l, new_i - 1)
    quicksort(a, new_i + 1, r)
```

Nos hypothèses seront les suivantes :
- Le vecteur à trier est une permutation des nombres de 1 à N.
- Le vecteur à trier est choisi uniformément aléatoirement parmi les $N!$ permutations de $1, \ldots, N$.
- On choisit le pivot i toujours, disons, tout à droite du vecteur ($i = r$). Ceci permet simplement de fixer les idées.

Soit X_N le nombre de comparaisons entre éléments du vecteur effectuées par quicksort sur un vecteur de taille N. Nous allons calculer l'espérance (moyenne) $E[X_N]$ de la variable aléatoire X_N.

Décomposons

$$X_N = Y_N + Z_N$$

où Y_N est le nombre de comparaisons effectuées pendant le partitionnement et Z_N est le nombre de comparaisons effectuées après le partitionnement, dans la partie récursive.

Notons que le nombre de comparaisons effectuées pendant le partitionnement est toujours $N-1$. Par conséquent, à N fixé, la variable aléatoire Y_N est constante, égale à $N-1$. Donc on a

$$E[Y_N] = N - 1\,.$$

Par linéarité de l'espérance,

$$\begin{aligned} E[X_N] &= E[Y_N] + E[Z_N] \\ &= (N-1) + E[Z_N] \end{aligned}$$

Pour chaque $k = 0, \ldots, N-1$, considérons l'événement "le rang du pivot est k". Ces N événements partitionnement l'espace fondamental. Par choix de la distribution initiale, ces événements ont tous la même probabilité, a savoir : $1/N$. La distribution conditionnelle sur chacun de ces évènements est de nouveau une distribution uniforme. Par ce qui précède, on peut calculer l'espérance de Z_N comme suit :

$$\begin{aligned} E[Z_N] &= \sum_{k=0}^{N-1} P[\text{rang du pivot est } k] \cdot E[Z_N \mid \text{rang du pivot est } k] \\ &= (N-1) + \sum_{k=0}^{N-1} \frac{1}{N} \cdot (E[X_k] + E[X_{N-1-k}]) \, . \end{aligned}$$

Posons maintenant $C_N := E[X_N]$. On trouve la récurrence

$$C_N = (N-1) + \frac{2}{N} \sum_{k=0}^{N-1} c_k \quad \forall N \geq 1; \quad c_0 = 0 \, .$$

Soit $C(x) := \sum_{N=0}^{\infty} c_N x^N$ la FGO de $(c_0, c_1, c_2, \ldots) = (0, c_1, c_2, \ldots)$. En multipliant l'équation de récurrence par N, on obtient :

$$NC_N = N(N-1) + 2 \sum_{k=0}^{N-1} c_k \quad \forall N \in \mathbb{N} \, .$$

En sommant pour $N \in \mathbb{N}$:

$$\sum_{N=0}^{\infty} NC_N x^N = \sum_{N=0}^{\infty} N(N-1)x^N + 2 \sum_{N=0}^{\infty} \left(\sum_{k=0}^{N-1} c_k \right) x^N \, .$$

Nous allons maintenant utiliser les résulats de base sur les FGO obtenus précédemment, voir en particulier le Théorème 3.8, pour exprimer chacun des termes ci-dessus :

- $\sum_{N=0}^{\infty} NC_N x^N$ est la FGO de $(0c_0, 1c_1, 2c_2, \ldots)$, donc $xC'(x)$.
- $\sum_{N=0}^{\infty} \left(\sum_{i=0}^{N-1} c_i \right) x^N$ est la FGO de $(0, c_0, c_0 + c_1, \ldots)$, donc $\frac{x}{1-x} C(x)$
- $\sum_{N=1}^{\infty} \frac{N(N-1)}{x}^N$ est 2 *fois* la FGO de $\left(\binom{n}{2} \right)_{n \in \mathbb{N}}$, donc $2 \cdot \frac{x^2}{(1-x)^3}$.

En remplaçant dans l'équation ci-dessus, on trouve une équation différentielle linéaire ordinaire :

$$xC'(x) = 2\frac{x^2}{(1-x)^3} + 2\frac{x}{1-x} C(x) \, .$$

Résolvons cette équation différentielle par la méthode des facteurs intégrants :

$$\begin{aligned}
xC'(x) &= 2\frac{x^2}{(1-x)^3} + 2\frac{x}{1-x}C(x) \\
\underset{x\neq 0}{\iff} C'(x) - \frac{2}{1-x}C(x) &= 2\frac{x}{(1-x)^3} \\
\iff (1-x)^2C'(x) - 2(1-x)C(x) &= 2\frac{x}{1-x} \\
\iff \left[(1-x)^2C(x)\right]' &= 2\frac{x}{1-x} \\
\iff (1-x)^2C(x) &= \int 2\frac{x}{1-x}\mathrm{d}x \\
\iff (1-x)^2C(x) &= 2\ln\frac{1}{1-x} - 2x + \mathrm{CST} \quad \text{avec CST} = 0 \text{ car } C(0) = 0
\end{aligned}$$

Finalement, on trouve

$$C(x) = \frac{2}{(1-x)^2}\ln\frac{1}{1-x} - \frac{2x}{(1-x)^2}\,.$$

Théorème 3.14. *Le nombre moyen de comparaisons entre éléments effectuées par Quicksort pour trier une permutation aléatoire des nombres $1, \ldots, N$ est exactement :*

$$C_N = [x^N]C(x) = 2(N+1)(H_{N+1} - 1) - 2N\,.$$

Démonstration. Par la Proposition 3.11,

$$\frac{1}{1-x}\ln\frac{1}{1-x}$$

est la FGO de $(H_0, H_1, H_2, \ldots, H_N, \ldots)$, où $H_N = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N}$ et $H_0 = 0$. Donc,

$$\frac{1}{1-x^2}\ln\frac{1}{1-x}$$

est la FGO de $(H_0, H_0 + H_1, \ldots, H_0 + H_1 + \ldots + H_N, \ldots)$. Or,

$$\begin{aligned}
\sum_{k=0}^{N} H_k = \sum_{k=1}^{N} H_k &= 1 + \left(1 + \frac{1}{2}\right) + \ldots + \left(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N}\right) \\
&= 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N} + \\
&\quad 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N} + \\
&\quad 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N} + \\
&\quad \vdots \qquad\qquad\qquad \vdots \\
&\quad 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{N} - N \\
&= (N+1)H_N - N \\
&= (N+1)(H_{N+1} - 1)\,.
\end{aligned}$$

De plus,

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

est la FGO de $(0, 1, 2, 3, \ldots, N, \ldots)$. En sommant et multipliant par deux, on conclut de ce qui précède :

$$c_N = [x^N]C(x) = [x^N]\frac{2}{(1-x)^2}\ln\frac{1}{1-x} - \frac{2x}{(1-x)^2} = 2(N+1)(H_{N+1}-1) - 2N\,.$$

□

Remarque 3.15. On verra plus tard que $H_N \sim N \ln N$, donc en particulier

$$E[X_N] \sim 2N \ln N\,.$$

En déployant des efforts supplémentaires, Knuth a pu montrer

$$\mathrm{Var}[X_N] \sim N^2\left(7 - \frac{2\pi^2}{3}\right)\,.$$

Rappelons l'*inégalité de Chebyshev* :

$$P[|X - E[X]| \geqslant a] \leqslant \frac{\mathrm{Var}[X]}{a^2}\,.$$

En appliquant cette inégalité à la variable aléatoire X_N, on voit

$$P[|X_N - E[X_N]| \geq KN] \leqslant \frac{\mathrm{Var}[X_N]}{K^2N^2} \sim \frac{7 - \frac{2\pi^2}{3}}{K^2}\,.$$

Donc la probabilité que X_N s'écarte fort de sa moyenne est extrêmement faible. Ceci explique pourquoi Quicksort se montre si rapide en pratique. (Alors que la complexité au pire cas est $\Omega(N^2)$.)

3.4.2 Un problème de monnaie

Nous terminons notre bref tour des applications des fonctions génératrices ordinaires avec le problème suivant, dû à Polyà :

> *De combien de manières peut-on rendre n eurocents de monnaie avec des pièces de 1, 2, 5 et 10 eurocents ?*

Soit $A(x) := \sum_{n=0}^{\infty} a_n x^n$ la FGO de la suite recherchée. Alors

$$A(x) = \left(\sum_{n_1=0}^{\infty} x^{n_1}\right)\left(\sum_{n_2=0}^{\infty} x^{2n_2}\right)\left(\sum_{n_5=0}^{\infty} x^{5n_5}\right)\left(\sum_{n_{10}=0}^{\infty} x^{10n_{10}}\right)\,,$$

et donc

$$A(x) = \frac{1}{1-x}\cdot\frac{1}{1-x^2}\cdot\frac{1}{1-x^5}\cdot\frac{1}{1-x^{10}}\,!$$

Remarquez le peu d'efforts à fournir pour trouver une expression de la FGO $A(x)$. Maintenant, comme extraire les coefficients a_n ? On a

$$A(x) = \frac{1+x+x^2+\ldots+x^9}{1-x^{10}}\cdot\frac{1+x^2+\ldots+x^8}{1-x^{10}}\cdot\frac{1+x^5}{1-x^{10}}\cdot\frac{1}{1-x^{10}}\,.$$

Maintenant, on peut allègrement effectuer le produit des numérateurs. Le numérateur résultant est un polynôme de degré 22, que nous noterons $\sum_{i=0}^{22} c_i x^i$. Reprenons :

$$A(x) = \frac{\sum_{i=0}^{22} c_i x^i}{(1-x^{10})^4} = \sum_{i=0}^{22} c_i \frac{x^i}{(1-x^{10})^4} ,$$

avec

$$c = (1,1,2,2,3,4,5,6,7,8,7,8,7,8,7,6,5,4,3,2,2,1,1) .$$

On sait que $\frac{x^3}{(1-x)^4}$ est la FGO de $\left(\binom{n}{3}\right)_{n\in\mathbb{N}}$ (voir Proposition 3.9). Donc $\frac{1}{(1-x)^4}$ est la FGO de $\left(\binom{n+3}{3}\right)_{n\in\mathbb{N}}$.

On va se baser là-dessus pour extraire les coefficients :

$$\frac{1}{(1-x)^4} = \sum_{k=0}^{\infty} \binom{k+3}{3} x^k \Longrightarrow \frac{1}{(1-x^{10})^4} = \sum_{k=0}^{\infty} \binom{k+3}{3} x^{10k} ,$$

donc

$$[x^{10k}] \frac{1}{(1-x^{10})^4} = \binom{k+3}{3}$$

puis

$$[x^n] \frac{1}{(1-x^{10})^4} = \begin{cases} \binom{\frac{n}{10}+3}{3} & \text{si } 10 \mid n \\ 0 & \text{si } 10 \nmid n \end{cases}$$

En posant $c_i = 0$ pour $i \in \{23,\dots,29\}$, et en utilisant le fait que $\binom{p}{3} = 0$ pour $p < 3$, on peut écrire la formule suivante pour a_n :

$$a_n = [x^n]A(x) = c_t \binom{\frac{n-t}{10}+3}{3} + c_{t+10} \binom{\frac{n-t}{10}+2}{3} + c_{t+20} \binom{\frac{n-t}{10}+1}{3} ,$$

où t est le reste de la division de n par 10, c'est-à-dire $t \equiv n \pmod{10}$ et $t \in \{0,\dots,9\}$.

Exemple 3.16. Pour $n = 10$, la formule donne

$$a_{10} = \binom{4}{3} + 7 \cdot \binom{3}{3} + 0 = 4 + 7 = 11 ,$$

ce qui est bien correct (exercice : compter le nombre de manières de rendre 10 eurocents de monnaie avec des pièces de 1, 2, 5 et 10 et vérifier que c'est bien 11 comme le prédit notre formule.)

3.5 Fonctions génératrices exponentielles : théorie de base

Définition 3.17 (Fonction génératrice exponentielle)**.** La *fonction génératrice exponentielle* (FGE) de la suite

$$(a_n)_{n\in\mathbb{N}} = (a_0, a_1, a_2, \dots)$$

est définie par

$$A(x) := \sum_{n=0}^{\infty} a_n \frac{x^n}{n!} .$$

On écrit :

$$n![x^n]A(x) = a_n .$$

Exemple 3.18 (Par calcul direct)**.** La FGE de $(1,1,1,\ldots) = \left(\binom{n}{0}\right)_{n\in\mathbb{N}}$ est

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} = e^x \,.$$

Généralisons : la FGE de $\left(\binom{n}{k}\right)_{n\in\mathbb{N}}$ est

$$\sum_{n=k}^{\infty} \binom{n}{k} \frac{x^n}{n!} = \sum_{n=k}^{\infty} \frac{n!}{k!(n-k)!} \frac{x^n}{n!} = \frac{x^k}{k!} \sum_{n=0}^{\infty} \frac{x^n}{n!} = \frac{x^k}{k!} e^x \,.$$

La FGE de $(1,1,2,6,24,\ldots,n!,\ldots) = (n!)_{n\in\mathbb{N}}$ est

$$\sum_{n=0}^{\infty} n! \frac{x^n}{n!} = \frac{1}{1-x} \,.$$

Remarquons que la FGO de la suite $(n!)_{n\in\mathbb{N}}$, contrairement à sa FGE, ne converge que pour $x = 0$. Ceci est un des avantages des FGE. Nous verrons plus loin que les FGE se prêtent mieux au comptage de structure étiquetées, alors que les FGO se prêtent mieux au comptage de structures non étiquetées.

Le résultat suivant est le pendant du Théorème 3.8, pour les fonctions génératrices exponentielles.

Théorème 3.19. *Soient $A(x)$ la FGE de $(a_n)_{n\in\mathbb{N}}$ et $B(x)$ la FGE de $(b_n)_{n\in\mathbb{N}}$. Alors :*

(i) $A(x) + B(x)$ *est la FGE de* $(a_0 + b_0, a_1 + b_1, \ldots, a_n + b_n, \ldots)$

(ii) $\int_0^x A(t)\mathrm{d}t$ *est la FGE de* $(0, a_0, a_1, a_2, \ldots, a_{n-1}, \ldots)$

(iii) $xA(x)$ *est la FGE de* $(0, a_0, 2a_1, 3a_2, \ldots, na_{n-1}, \ldots)$

(iv) $A'(x)$ *est la FGE de* $(a_1, a_2, a_3, a_4, \ldots, a_{n+1}, \ldots)$

(v) $\frac{A(x)-A(0)}{x}$ *est la FGE de* $(a_1, \frac{a_2}{2}, \frac{a_3}{3}, \ldots, \frac{a_{n+1}}{n+1}, \ldots)$

(vi) $A'(x) - A(x)$ *est la FGE de* $(a_1 - a_0, a_2 - a_1, \ldots, a_{n+1} - a_n, \ldots)$

(vii) $A(x)B(x)$ *est la FGE de* $(a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + 2a_1b_1 + a_2b_0, \ldots, \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}, \ldots)$

(viii) $e^x A(x)$ *est la FGE de* $(a_0, a_0 + a_1, a_0 + 2a_1 + a_2, \ldots, \sum_{k=0}^{n} \binom{n}{k} a_k, \ldots)$

3.6 Fonctions génératrices exponentielles : application

Nous désirons calculer la somme

$$S_t(n) := \sum_{0\leqslant k<n} k^t = 0^t + 1^t + \cdots + (n-1)^t$$

des puissances t-èmes des naturels de 0 à $n-1$, pour $t \in \mathbb{N}$.

Exemple 3.20. Pour $t = 0$,

$$S_0(n) = 0^0 + 1^0 + \ldots + (n-1)^0 = n$$

(on a posé $0^0 = 1$). Pour $t = 1$,

$$S_1(n) = 0^1 + 1^1 + \ldots + (n-1)^1 = \frac{n(n-1)}{2} \,.$$

Nous allons obtenir une formule générale pour $S_t(n)$ qui fait intervenir les nombres de Bernouilli, voir Théorème 3.21 ci-dessous.

La suite des *nombres de Bernouilli* $(B_k)_{k\in\mathbb{N}} = (B_0, B_1, B_2, \ldots)$ est définie comme l'unique suite vérifiant

$$x = \left(B_0 + B_1\frac{x}{1!} + B_2\frac{x^2}{2!} + B_3\frac{x^3}{3!} + \cdots\right)\left(\frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots\right) . \tag{3.3}$$

En d'autre termes, cette suite est telle que sa FGE est

$$\frac{x}{\frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{6!} + \cdots} = \frac{x}{e^x - 1} .$$

Donc, pour $k \in \mathbb{N}$, le k-ème nombre de Bernouilli vérifie

$$B_k := k![x^k]\frac{x}{e^x - 1} .$$

On peut calculer B_k en identifiant les coefficients de x^{k+1} dans les deux membres de (3.3). Ce calcul fait intervenir $B_0, \ldots, B_{k-1}$, que l'on suppose avoir calculé avant. Par exemple, pour $0 \leqslant k \leqslant 3$, on trouve

$$\begin{aligned} 1 &= B_0 \\ 0 &= \frac{1}{2}B_0 + B_1 \\ 0 &= \frac{1}{6}B_0 + \frac{1}{2}B_1 + \frac{1}{2}B_2 \\ 0 &= \frac{1}{24}B_0 + \frac{1}{6}B_1 + \frac{1}{4}B_2 + \frac{1}{6}B_3 , \end{aligned}$$

ce qui donne $B_0 = 1$, $B_1 = -1/2$, $B_2 = 1/6$ et $B_3 = 0$.

Théorème 3.21. *Pour tous $t, n \in \mathbb{N}$:*

$$\sum_{0\leqslant k<n} k^t = \frac{1}{t+1}\sum_{k=0}^{t}\binom{t+1}{k}B_k n^{t+1-k} .$$

Démonstration. A n fixé, la FGE de la suite $(S_0(n), S_1(n), S_2(n), \ldots) = (S_t(n))_{t\in\mathbb{N}}$ s'écrit

$$\begin{aligned} \sum_{t=0}^{\infty} S_t(n)\frac{x^t}{t!} &= \sum_{t=0}^{\infty}\left(\sum_{0\leqslant k<n} k^t\right)\frac{x^t}{t!} \\ &= \sum_{0\leqslant k<n}\sum_{t=0}^{\infty}\frac{(kx)^t}{t!} \\ &= \sum_{0\leqslant k<n} e^{kx} \\ &= 1 + e^x + (e^x)^2 + \ldots (e^x)^{n-1} \\ &= \frac{e^{nx} - 1}{e^x - 1} \\ &= \frac{x}{e^x - 1}\cdot\frac{e^{nx} - 1}{x} . \end{aligned}$$

Dans cette dernière expression, le facteur de gauche est par définition la FGE de la suite des nombres de Bernouilli $(B_0, B_1, B_2, \ldots, B_k, \ldots)$. Le facteur de droite, est quant à lui la FGE de la suite $(n, \frac{n^2}{2}, \frac{n^3}{3}, \ldots, \frac{n^{\ell+1}}{\ell+1}, \ldots)$.

La FGE de la suite recherchée étant le produit des FGE des deux suites $(B_k)_{k\in\mathbb{N}}$ et $(\frac{n^{\ell+1}}{\ell+1})_{\ell\in\mathbb{N}}$, la suite recherchée $(S_t(n))_{n\in\mathbb{N}}$ peut s'obtenir en calculant la convolution binomiale de ces deux suites (voir Théorème 3.19(vii)) :

$$\begin{aligned} S_t(n) &= \sum_{k=0}^{t} \binom{t}{k} B_k \frac{n^{t+1-k}}{t+1-k} \\ &= \sum_{k=0}^{t} \frac{t!}{k!(t-k)!} B_k \frac{n^{t+1-k}}{t+1-k} \\ &= \frac{1}{t+1} \sum_{k=0}^{t} \binom{t+1}{k} B_k n^{t+1-k} \,. \end{aligned}$$

□

3.7 Exercices

Exercice 3.1. Que vaut

$$\sum_{n=0}^{\infty} H_n \frac{1}{10^n} \quad ?$$

(Rappel : H_n est le n-ème nombre harmonique.)

Exercice 3.2. Trouver les fonctions génératrices ordinaire et exponentielle de $(2^n + 3^n)_{n\in\mathbb{N}}$, en forme close.

Exercice 3.3. Un collectionneur excentrique rafolle des pavages de rectangles $2 \times n$ par des dominos verticaux 2×1 et horizontaux 1×2. Il paye sans hésiter 4€ par domino vertical et 1€ par domino horizontal. Pour combien de pavages sera-t-il prêt à payer n€ ?

Exercice 3.4. Déterminer la fonction génératrice ordinaire $S(x)$ telle que

$$[x^n]S(x) = \sum_k \binom{r}{k} \binom{r}{n-2k} .$$

Exercice 3.5. Résoudre la récurrence

$$\begin{aligned} &a_n = a_{n-1} + 2a_{n-2} + \cdots + na_0 \quad \forall n \geqslant 1 \\ &a_0 = 1 \end{aligned}$$

en utilisant les fonctions génératrices ordinaires.

Exercice 3.6. Résoudre la récurrence

$$\begin{aligned} &a_n = -2na_{n-1} + \sum_k \binom{n}{k} a_k a_{n-k} \quad \forall n \geqslant 2 \\ &a_0 = 0, \quad a_1 = 1 \end{aligned}$$

en utilisant les fonctions génératrices exponentielles.

Exercice 3.7. (Examen janvier 2011.) Calculer la somme de chacune des séries suivantes.

a) $\displaystyle\sum_{n=0}^{\infty} \frac{H_n}{2^n}$

b) $\displaystyle\sum_{n=0}^{\infty} \binom{n}{2} \frac{1}{10^n}$

Exercice 3.8. (Examen janvier 2011.) Pour $n \in \mathbb{N}$, désignons par a_n le nombre de manières de rendre n eurocents de monnaie avec des pièces de 1, 5 et 10 eurocents.

a) Déterminer a_n pour $n \in \{0, \ldots, 10\}$.

b) Trouver la fonction génératrice ordinaire $A(x)$ de la suite $(a_n)_{n\in\mathbb{N}}$.

c) Déterminer a_n pour $n \in \{2010, 2011\}$.

Exercice 3.9. (Examen août 2011.) Calculer la somme de chacune des séries suivantes.

a) $\displaystyle\sum_{n=1}^{\infty} \frac{1}{2^n}$

b) $\displaystyle\sum_{n=1}^{\infty} \frac{n}{2^n}$

c) $\displaystyle\sum_{n=1}^{\infty} \frac{1}{n2^n}$

Chapitre 4

Comportements asymptotiques

4.1 Nombres harmoniques et constante d'Euler

Pour rappel, le n-ème nombre harmonique est défini par

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} .$$

Ces nombres apparaissent dans de nombreux contextes (dans ce syllabus, nous les avons rencontrés dans l'analyse de Quicksort, voir plus haut).

Ici, nous allons montrer :

(i) $H_n \sim \ln(n)$, c'est-à-dire l'erreur relative commise quand on remplace H_n par $\ln(n)$ tend vers 0 pour $n \to \infty$;

(ii) $\lim_{n\to\infty} H_n - \ln(n) = \gamma$, c'est-à-dire l'erreur absolue commise quand on remplace H_n par $\ln(n)$ tend vers une constante γ pour $n \to \infty$; cette constante est appelée *constante d'Euler*.

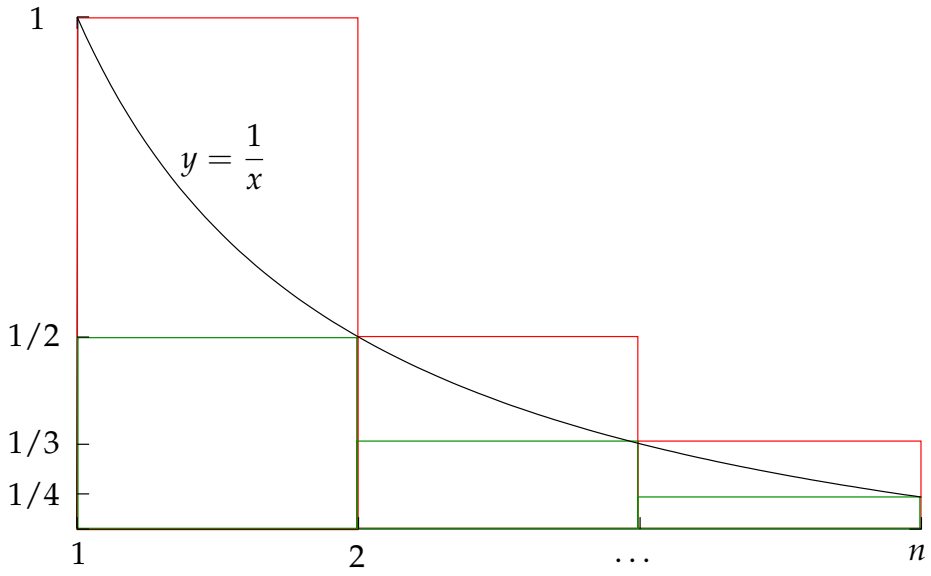
Définition 4.1 (Erreur absolue / erreur relative)**.** Soient x, y deux réels, avec $x \neq 0$. L'erreur *relative* commise en remplaçant x par y est

$$|x - y| .$$

L'erreur *absolue* commise en remplaçant x par y est

$$\left| \frac{x - y}{x} \right| .$$

Remarque 4.2 (Série harmonique)**.** $H_\infty = \sum_{k=0}^{\infty} \frac{1}{k} = \infty$, c'est-à-dire $\lim_{n\to\infty} H_n = \infty$.



Sur le schéma ci-dessus, nous pouvons distinguer 3 aires différentes :

1. L'aire (verte) des rectangles sous la courbe :

$$\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} = H_n - 1\,;$$

2. L'aire sous la courbe $y = 1/x$:

$$\int_1^n \frac{1}{t}\mathrm{d}t = \ln(n)\,;$$

3. L'aire (rouge) des rectangles au-dessus de la courbe :

$$1 + \frac{1}{2} + \ldots + \frac{1}{n-1} = H_{n-1}\,.$$

En comparant ces aires, il est évident que

$$H_n - 1 < \ln(n) < H_{n-1}\,.$$

Comme ceci est vrai pour tout $n \geqslant 2$, on a :

$$\ln(n+1) < H_n < \ln(n) + 1 \Longrightarrow \ln(n) < H_n < \ln(n) + 1$$

et donc

$$\lim_{n\to\infty} \frac{H_n}{\ln(n)} = 1\,,$$

c'est-à-dire $H_n \sim \ln(n)$.

Remarque 4.3. On voit, de part l'inégalité $H_n < \ln(n) + 1$ que la série harmonique $\sum_{k=1}^{\infty} \frac{1}{k}$ diverge *logarithmiquement*, donc très lentement. Bien que H_n tend vers $+\infty$ quand $n \to \infty$, pour avoir $H_n > 10$ il est nécessaire que $\ln(n) + 1 \geqslant 10$ donc $n \geqslant 8104$.

Pour montrer que $H_n - \ln(n)$ tend vers une constante quand $n \to \infty$, posons

$$a_n := H_n - \ln(n)$$

Etant donné que $H_n > \ln(n)$, on a $a_n > 0$. Donc a_n est l'erreur absolue commise en remplaçant H_n par $\ln(n)$. De plus, la suite $(a_n)_{n\in\mathbb{N}}$ est (strictement) décroissante, car :

$$\begin{aligned} a_{n+1} - a_n &= H_{n+1} - \ln(n+1) - H_n + \ln(n) \\ &= \frac{1}{n+1} - \underbrace{\ln(n+1) - \ln(n)}_{=\int_n^{n+1} \frac{1}{t}\mathrm{d}t} \\ &< 0 \quad \text{(géométriquement, par comparaison des aires)} . \end{aligned}$$

Donc

$$a_1 > a_2 > a_3 > \cdots > a_n > a_{n+1} > \cdots > 0 .$$

La suite $(a_n)_{n\in\mathbb{N}}$, étant minorée (par 0) et décroissante, converge. Posons

$$\gamma := \lim_{n\to\infty} \underbrace{(H_n - \ln(n))}_{a_n} .$$

On peut calculer γ numériquement :

$$\gamma = 0,5772156649\ldots$$

Remarque 4.4. On peut montrer qu'en fait

$$H_n = \ln(n) + \gamma + \frac{1}{2n} - \frac{1}{12n^2} + \frac{1}{120n^4} - \epsilon_n \qquad \text{avec } 0 < \epsilon_n < \frac{1}{252n^6} .$$

En particulier : $nH_n = n\ln(n) + n\gamma + \Theta(1)$.

4.2 Factorielles et formule de Stirling

Vers 1730, de Moivre a montré $n! \sim C\sqrt{n}\left(\frac{n}{\mathrm{e}}\right)^n$. Stirling a ensuite obtenu $C = \sqrt{2\pi}$, en utilisant la formule de Wallis ci-dessous, qui établit un lien surprenant entre $n!$ et π.

Théorème 4.5 (Formule de Wallis)**.**

$$\frac{\pi}{2} = \lim_{n\to\infty} \frac{2\cdot 2\cdot 4\cdot 4\cdots 2n\cdot 2n}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdots (2n-1)\cdot(2n-1)\cdot(2n+1)}$$

Démonstration. Pour $m \in \mathbb{N}$, posons

$$I_m := \int_0^{\pi/2} \sin^m x \,\mathrm{d}x .$$

Les deux premières valeurs de m donnent

$$I_0 := \int_0^{\pi/2} \sin^0 x \,\mathrm{d}x = \frac{\pi}{2} \quad \text{et} \quad I_1 := \int_0^{\pi/2} \sin^1 x \,\mathrm{d}x = 1 .$$

Pour $m \geqslant 2$,

$$\begin{aligned} I_m &= \int_0^{\pi/2} \sin^{m-1} x \cdot \sin x \, \mathrm{d}x \\ &= \Big[\sin^{m-1} x \cdot (-1)\cos x\Big]_0^{\pi/2} - \int_0^{\pi/2} (m-1)\sin^{m-2} x \cdot \cos x \cdot (-1)\cos x \, \mathrm{d}x \\ &= (m-1)\int_0^{\pi/2} \sin^{m-2} x \cdot (1-\sin^2 x)\, \mathrm{d}x \\ &= (m-1)\int_0^{\pi/2} \sin^{m-2} x \, \mathrm{d}x - (m-1)\int_0^{\pi/2} \sin^m x \, \mathrm{d}x \\ &= (m-1)I_{m-2} - (m-1)I_m \, . \end{aligned}$$

Par conséquent,

$$I_m = \frac{m-1}{m} I_{m-2} \, . \tag{4.1}$$

On trouve alors

$$I_{2n} = \frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \cdots \cdot \frac{3}{4} \cdot \frac{1}{2} \cdot \underbrace{I_0}_{=\pi/2}$$

et

$$I_{2n+1} = \frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdot \cdots \frac{4}{5} \cdot \frac{2}{3} \cdot \underbrace{I_1}_{=1} \, .$$

Pour $x \in [0, \pi/2]$,

$$0 \leqslant \sin x \leqslant 1 \implies \sin^{2n+1} x \leqslant \sin^{2n} x \leqslant \sin^{2n-1} x \, .$$

En intégrant sur $[0, \pi/2]$, on trouve

$$I_{2n+1} \leqslant I_{2n} \leqslant I_{2n-1} \implies 1 \leqslant \frac{I_{2n}}{I_{2n+1}} \leqslant \frac{I_{2n-1}}{I_{2n+1}} \, .$$

Par l'équation (4.1) ci-dessus, la dernière fraction vaut $(2n+1)/2n$ (poser $m = 2n+1$). En passant à la limite, on trouve

$$\lim_{n\to\infty} \frac{I_{2n}}{I_{2n+1}} = 1$$

c'est-à-dire

$$\lim_{n\to\infty} \frac{\frac{2n-1}{2n} \cdot \frac{2n-3}{2n-2} \cdot \cdots \cdot \frac{3}{4} \cdot \frac{1}{2} \cdot \frac{\pi}{2}}{\frac{2n}{2n+1} \cdot \frac{2n-2}{2n-1} \cdots \frac{4}{5} \cdot \frac{2}{3} \cdot 1} = 1$$

ou encore

$$\frac{\pi}{2} \lim_{n\to\infty} \frac{(2n+1)\cdot(2n-1)\cdot(2n-1)\cdots 5\cdot 5\cdot 3\cdot 3\cdot 1}{(2n)\cdot(2n)\cdot(2n-2)\cdot(2n-2)\cdots 4\cdot 4\cdot 2\cdot 2} = 1 \, .$$

En inversant les fractions dans la dernière égalité, on obtient la formule de Wallis. □

Repartons de la formule de Wallis, dans le but d'obtenir une formule approchée pour les

coefficients “centraux” du triangle de Pascal.

$$\begin{aligned}\frac{\pi}{2} &= \lim_{n\to\infty} \frac{2\cdot 2\cdot 4\cdot 4\cdot\cdots 2n\cdot 2n}{1\cdot 3\cdot 3\cdot 5\cdot 5\cdot\cdots(2n-1)\cdot(2n-1)\cdot(2n+1)} \\ &= \lim_{n\to\infty} \frac{(2n)^4\cdot\ldots\cdot 4^4\cdot 2^4}{(2n+1)\cdot(2n)^2\cdot(2n-1)^2\cdot\ldots\cdot 5^2\cdot 4^2\cdot 3^2\cdot 2^2} \\ &= \lim_{n\to\infty} \frac{1}{2n+1}\frac{\overbrace{[2\cdot 4\cdot 6\cdot\ldots\cdot(2n)}^{n \text{ facteurs pairs}}]^4}{[(2n)!]^2} \\ &= \lim_{n\to\infty} \frac{2^{4n}}{2n+1}\cdot\frac{(n!)^4}{[(2n)!]^2}\end{aligned}$$

De ceci, on tire :

$$1 = \lim_{n\to\infty} \frac{2}{\pi}\cdot\frac{2^{4n}}{2n+1}\cdot\frac{1}{\left[\frac{(2n)!}{n!n!}\right]^2}\,.$$

C’est-à-dire :

$$\binom{2n}{n}^2 \sim \frac{2}{\pi}\cdot\frac{2^{4n}}{2n+1} \sim \frac{2}{\pi}\cdot\frac{2^{4n}}{2n} \sim \frac{2^{4n}}{\pi n}\,.$$

En extrayant les racines carrées, on trouve la formule voulue :

$$\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}}$$

Remarque 4.6 (Fibonacci vs. Catalan)**.** Comme nous l’avons vu précédemment, les nombres de Fibonacci vérifient :

$$F_n \sim \frac{1}{\sqrt{5}}\varphi^n = \frac{1}{\sqrt{5}}(1,6180\ldots)^n.$$

En ce qui concerne les nombre de Catalan, la formule de Wallis nous donne :

$$C_{n+1} = \frac{1}{n+1}\binom{2n}{n} \sim \frac{4^n}{\sqrt{\pi}n^{3/2}}\,.$$

On voit alors que

$$C_n \gg F_n \qquad \text{pour } n \text{ grand.}$$

Comment obtenir la constante C dans la formule de de Moivre $n! \sim C\sqrt{n}(n/e)^n$?

D’une part, par la formule de Wallis on a obtenu :

$$\binom{2n}{n} \sim \frac{1}{\sqrt{\pi}}\frac{2^{2n}}{\sqrt{n}}$$

D’autre part, en utilisant la formule de de Moivre :

$$\binom{2n}{n} = \frac{(2n)!}{n!\,n!} \sim \frac{C\sqrt{2n}\left(\frac{2n}{e}\right)^{2n}}{C^2 n\left(\frac{n}{e}\right)^{2n}} = \frac{\sqrt{2}}{C}\frac{2^{2n}}{\sqrt{n}}\,.$$

En comparant les expressions asymptotiques pour $\binom{2n}{n}$, on doit avoir $\sqrt{2}\frac{1}{C} = \frac{1}{\sqrt{\pi}}$, c’est-à-dire $C = \sqrt{2\pi}$. On obtient la formule asymptotique suivante.

Théorème 4.7 (formule de Stirling)**.**

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n .$$

De manière plus précise,

Théorème 4.8. *Pour tout $n \in \mathbb{N}$:*

$$n! = \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\varepsilon_n}$$

pour un certain ε_n avec

$$\frac{1}{12n+1} < \varepsilon_n < \frac{1}{12n} .$$

Parce que l'exponentielle en base e est continue et croissante, ce dernier théorème est équivalent à l'inégalité suivante :

$$\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12n+1}} < n! < \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n \mathrm{e}^{\frac{1}{12n}} .$$

Remarque 4.9. L'erreur relative commise en remplaçant $n!$ par $\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n$ vaut

$$\left|\frac{n! - \sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n}{n!}\right| \approx \frac{1}{12n} \qquad (\underset{n\to\infty}{\longrightarrow} 0)$$

Pour conclure cette section sur la formule de Stirling, voici un tableau avec quelques valeurs numériques. Comme on peut le constater, l'erreur absolue commise en remplaçant $n!$ par $\sqrt{2\pi n}\left(\frac{n}{\mathrm{e}}\right)^n$ est assez conséquente. En vérité, il est difficile d'obtenir de très bonnes approximations de $n!$.

n	Approximation de Stirling	Erreur absolue	Erreur relative
1	$0,922\ldots$	$\approx 0,08$	$\approx 8\%$
2	$1,919\ldots$	$\approx 0,08$	$\approx 4\%$
5	$118,019\ldots$	≈ 2	$\approx 1,6\%$
100	$\approx 9,324 \cdot 10^{157}$	$\approx 1,7 \cdot 10^{155}$	$\approx 0,08\%$

4.3 Formule d'Euler-Mc Laurin

Commençons par retourner quelques pages en arrière. Nous avons vu :

$$0^t + 1^t + 2^t + \ldots + (n-1)^t = \frac{n^{t+1}}{t+1} + \sum_{k=1}^{t} \binom{t+1}{k} B_k\, n^{t+1-k} .$$

Posons $f(x) = x^t$. Remarquons que

$$\int_0^n f(x)\,\mathrm{d}x = \int_0^n x^t\,\mathrm{d}x = \frac{n^{t+1}}{t+1} .$$

La formule ci-dessus (celle qui fait intervenir les nombres de Bernouilli B_k) peut donc se lire :

$$\sum_{0 \leqslant k < n} f(k) = \int_0^n f(x) + \text{termes d'ordres inférieurs .}$$

Un autre exemple est l'approximation que l'on a obtenu pour les nombres harmoniques :

$$H_{n-1} = \ln n + \text{termes d'ordres inférieurs .}$$

Dans ce cas-ci, posons $f(x) = 1/x$. On trouve, de manière similaire :

$$\sum_{1 \leqslant k < n} f(k) = \int_1^n f(x)\mathrm{d}x + \text{termes d'ordres inférieurs .}$$

Il est naturel de se demander à quel point l'intégrale $\int_a^b f(x)\mathrm{d}x$ constitue une bonne approximation de la somme $\sum_{a \leqslant k < b} f(k)$, pour des fonctions f plus générales. C'est précisément l'intérêt de la formule d'Euler-Mc Laurin.

Théorème 4.10 (Formule d'Euler-Mc Laurin)**.** *Soient a, b des entiers tels que $a \leqslant b$. Soit m un entier avec $m \geqslant 1$. Soit $f : [a, b] \to \mathbb{R}$ une fonction telle que $\frac{\mathrm{d}f}{\mathrm{d}x}$, $\frac{\mathrm{d}^2 f}{\mathrm{d}x^2}$, …, $\frac{\mathrm{d}^m f}{\mathrm{d}x^m}$ existent et sont continues sur $[a, b]$. Alors,*

$$\sum_{a \leqslant k < b} f(k) = \int_a^b f(x)\mathrm{d}x + \sum_{k=1}^{m} \frac{B_k}{k!} \left[\frac{\mathrm{d}^{k-1} f}{\mathrm{d}x^{k-1}}(x) \right]_a^b + R_m \, .$$

Le reste R_m satisfait :

$$R_m = (-1)^{m+1} \int_a^b \frac{B_m(\{x\})}{m!} \frac{\mathrm{d}^m f}{\mathrm{d}x^m}(x)\mathrm{d}x \, ,$$

où $B_m(x)$ est le m-ème polynôme de Bernouilli,

$$B_m(x) := \sum_{k=0}^{m} \binom{m}{k} B_k \, x^{m-k}$$

et $\{x\} := x - \lfloor x \rfloor$ est la partie fractionnaire de x.

"Preuve" heuristique. La formule d'Euler-Mc Laurin est un dialogue entre deux "théories". D'une part, le calcul différentiel et intégral auquel nous sommes familiers (avec ses notions de dérivée, intégrale, ses ε et ses δ). D'autre part, ce que nous appelons le *calcul différentiel discret*. Comparons les deux théories :

	Calcul différentiel et intégral	Calcul différentiel discret
Opérateurs	$\int \longleftrightarrow D$	$\Sigma \longleftrightarrow \Delta$

On reconnaît les opérateurs d'intégration $\int$ et de sommation Σ. Les opérateurs D et Δ sont la dérivée usuelle, et la *dérivée discrète* :

$$Df(x) := \frac{\mathrm{d}}{\mathrm{d}x} f(x) = f'(x)$$
$$\Delta f(x) := f(x+1) - f(x) \, .$$

On a :

$$\left(\int D\right)(f) = \left(D\int\right)(f) = f$$

pour toute fonction dérivable f. Nous noterons $D^{-1} = \int$. De manière similaire, on peut vérifier :

$$(\Sigma\Delta)(f) = (\Delta\Sigma)(f)\,,$$

ce que nous notons $\Delta^{-1} = \Sigma$.

Développons f autour de 0 par la formule de Taylor :

$$f(x+\varepsilon) = f(x) + \frac{f'(x)}{1!}\varepsilon + \frac{f''(x)}{2!}\varepsilon^2 + \dots$$

puis prenons $\varepsilon = 1$:

$$\begin{aligned}
\Delta f(x) &= f(x+1) - f(x) \\
&= \frac{f'(x)}{1!} + \frac{f''(x)}{2!} + \frac{f'''(x)}{3!} + \dots \\
&= \left(\frac{D}{1!} + \frac{D^2}{2!} + \frac{D^3}{3!} + \dots\right) f(x) \\
&= \left(e^D - 1\right) f(x)\,.
\end{aligned}$$

Par conséquent, on a l'égalité entre opérateurs :

$$\Delta = e^D - 1\,.$$

En "inversant", on trouve

$$\Sigma = \Delta^{-1} = \frac{1}{e^D - 1}\,.$$

Poursuivons :

$$\begin{aligned}
\Sigma &= \frac{1}{D}\cdot\frac{D}{e^D-1} \\
&= \frac{1}{D}\cdot\left(B_0 + \frac{B_1}{1!}D + \frac{B_2}{2!}D^2 + \dots\right) \\
&= \frac{\overbrace{B_0}^{=1}}{D} + \frac{B_1}{1!} + \frac{B_2}{2!}D + \dots \\
&= \int + \frac{B_1}{1!} + \frac{B_2}{2!}D + \dots
\end{aligned}$$

On trouve finalement

$$\Sigma = \int + \sum_{k=1}^{\infty} \frac{B_k}{k!} D^{k-1}$$

et donc

$$\sum_{a\leqslant k<b} f(k) = \int_a^b f(x)\mathrm{d}x + \sum_{k=1}^{\infty} \frac{B_k}{k!}\left[\frac{\mathrm{d}^{k-1}f}{\mathrm{d}x^{k-1}}(x)\right]_a^b\,.$$

En tronquant la série, on obtient

$$\sum_{a\leqslant k<b} f(k) = \int_a^b f(x)\mathrm{d}x + \sum_{k=1}^{\infty} \frac{B_k}{k!}\left[\frac{\mathrm{d}^{k-1}f}{\mathrm{d}x^{k-1}}(x)\right]_a^b + \underbrace{R_m}_{\text{reste}}\,.$$

Nous arrêtons ici cet argument heuristique, qui n'est pas une preuve formelle, mais sur la base duquel une preuve formelle peut être construite (voir le livre *Concrete Mathematics* de R. Graham, D. Knuth et O. Patashnik). □

Exemple 4.11 (Approximation de $\ln(n!)$ et formule de Stirling)**.** Prenons $f(x) := \ln x$, $a := 1$, $b := n$ et $m := 2p$ (un nombre pair pas trop grand). Alors :

$$\int_a^b f(x)\mathrm{d}x = \int_1^n \ln x \,\mathrm{d}x = \left[x\ln x - x\right]_1^n = n\ln n - n + 1\,.$$

Pour $k \geqslant 2$:

$$\left[\frac{1}{k!}\frac{\mathrm{d}^{k-1}f}{\mathrm{d}x^{k-1}}(x)\right]_a^b = \left[\frac{1}{k!}(-1)^{k-2}(k-2)!\frac{1}{x^{k-1}}\right]_1^n = (-1)^{k-2}\frac{1}{k(k-1)n^{k-1}} - (-1)^{k-2}\frac{1}{k(k-1)}\,.$$

Par la formule d'Euler-Mc Laurin, on obtient alors :

$$\begin{aligned}
\ln((n-1)!) &= \sum_{1\leqslant k<n} \ln k \\
&= \sum_{a\leqslant k<b} f(k) \\
&= \int_a^b f(x)\mathrm{d}x + \sum_{k=1}^{m} B_k\left[\frac{1}{k!}\frac{\mathrm{d}^{k-1}f}{\mathrm{d}x^{k-1}}(x)\right]_a^b + R_m \\
&= (n\ln n - n + 1) + \Bigg[\underbrace{B_1}_{=-\frac{1}{2}}\ln x\Bigg]_1^n + \sum_{k=2}^{m} B_k\frac{(-1)^{k-2}}{k(k-1)}\left(\frac{1}{n^{k-1}} - 1\right) + R_m
\end{aligned}$$

On peut vérifier en utilisant
– $B_k = 0$ pour k impair ($k \geqslant 3$) et
– un *truc* pour évaluer R_m
que

$$\ln((n-1)!) = n\ln n - n - \frac{\ln n}{2} + \sigma + \sum_{l=1}^{p}\frac{B_{2l}}{2l(2l-1)n^{2l-1}} + \varphi_{p,n}\frac{B_{2p+2}}{(2p+2)(2p+1)n^{2p+1}}$$

où $0 < \varphi_{p,n} < 1$ et σ est la constante de Stirling (on sait que $e^\sigma = \sqrt{2\pi}$ par Wallis). Donc, en ajoutant $\ln n$ à chaque membre, on trouve :

$$\ln(n!) = n\ln n - n + \frac{\ln n}{2} + \sigma + \sum_{l=1}^{p}\frac{B_{2l}}{2l(2l-1)n^{2l-1}} + \varphi_{p,n}\frac{B_{2p+2}}{(2p+2)(2p+1)n^{2p+1}}$$

Pour $p = 2$ ($m = 4$), on trouve :

$$\ln(n!) = n\ln n - n + \frac{\ln n}{2} + \sigma + \frac{1}{6}\cdot\frac{1}{2(2-1)n^{2-1}} - \frac{1}{30}\cdot\frac{1}{4(4-1)n^{4-1}} + \underbrace{\text{reste}}_{O\left(\frac{1}{n^5}\right)}\,.$$

En réécrivant,

$$\ln(n!) = n\ln n - n + \frac{\ln n}{2} + \sigma + \frac{1}{12n} - \frac{1}{360n^3} + O\left(\frac{1}{n^5}\right)\,.$$

Remarque 4.12.

1. Les premiers nombres de Bernouilli sont : $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$.
2. Il n'est pas intéressant de prendre m grand car B_{2p+2} augmente au bout d'un moment.

4.4 La méthode analytique : nombres de Bell ordonnés

Nous terminons ce chapitre sur les comportements asymptotiques en voyant une nouvelle utilisation des fonctions génératrices. Précédemment, nous avons exploité les fonctions génératrices pour obtenir des formules explicites (ou formes closes) pour les termes de suites (nombres de Catalan, nombre de comparaisons moyen de Quicksort, etc...). Ici, nous allons tirer des informations asymptotiques sur une suite à partir de sa fonction génératrice, en utilisant l'analyse complexe. Pour cette suite, aucune formule explicite n'est connue.

Notre exemple est celui des *nombres de Bell ordonnés*, définis par :

$$\begin{aligned} b_n &:= \#\text{partitions ordonnées d'un ensemble de } n \text{ éléments (en classes non vides)} \\ &= \#\text{préordres totaux sur } [n] = \{1, 2, \ldots, n\} \,. \end{aligned}$$

Exemple 4.13. Pour $n = 1$, il y a 1 partition ordonnée :

$$(\{1\}) \,.$$

Pour $n = 2$, il y en a 3 :

$$(\{1,2\}), \quad (\{1\},\{2\}) \quad \text{et} \quad (\{2\},\{1\}) \,.$$

Pour $n = 3$, il y en a 13 :

$(\{1,2,3\})$	total : 1
$(\{1\},\{2,3\}), \quad \ldots, \quad (\{2,3\},\{1\})$	total : 6
$(\{1\},\{2\},\{3\}), \quad \ldots, \quad (\{3\},\{2\},\{1\})$	total : 6
	grand total : 13 .

Donc on trouve $b_1 = 1$, $b_2 = 3$ et $b_3 = 13$.

4.4.1 FGE des nombres de Bell ordonnés par la méthode symbolique

Pour obtenir la FGE de la suite $(b_n)_{n\in\mathbb{N}}$ nous allons utiliser la *méthode symbolique*. Cette méthode étudie des classes $\mathcal{O}$ d'objets étiquetés.

Exemple 4.14.
- La classe des permutations : $\mathcal{P} = \{\epsilon, 1, 12, 21, 123, 132, 213, 231, 312, 321, \ldots\}$.
- La classe des cycles : $\mathcal{C} = \{(1), (1,2), (1,2,3), (3,2,1), \ldots\}$.
- La classe des ensembles non vides : $\mathcal{E} = \{\{1\}, \{1,2\}, \{1,2,3\}, \ldots\}$.

Ci-dessus, ϵ désigne l'*objet vide*. De plus $(1,2,3) = (2,3,1) = (3,1,2)$ et $(3,2,1) = (2,1,3) = (1,3,2)$.

Chaque objet $o \in \mathcal{O}$:
- est constitué d'éléments appelés *atomes* ;
- possède une *taille*, notée $|o|$ et définie comme le nombre d'atomes constituant o ;
- est *étiqueté* dans le sens que ses atomes portent les étiquettes 1, 2, ..., n.

La FGE de $\mathcal{O}$ est définie par

$$O(x) := \sum_{o\in\mathcal{O}} \frac{x^{|o|}}{|o|!} = \sum_{n=0}^{\infty} (\#\text{ d'objets de taille } n \text{ dans } \mathcal{O}) \frac{x^n}{n!} \,.$$

Exemple 4.15. (suite)
- FGE de la classe $\mathcal{P}$ des permutations : $P(x) = \sum_{n=0}^{\infty} n! \frac{x}{n!} = \frac{1}{1-x}$.

– FGE de la classe $\mathcal{C}$ des cycles : $C(x) = \sum_{n=1}^{\infty}(n-1)!\frac{x^n}{n!} = \sum_{n=1}^{\infty}\frac{x^n}{n} = \ln\left(\frac{1}{1-x}\right)$.

– FGE de la classe $\mathcal{E}$ des ensembles non vides : $E(x) = \sum_{n=1}^{\infty}\frac{x^n}{n!} = \mathrm{e}^x - 1$.

Si $\mathcal{A}$ et $\mathcal{B}$ sont deux classes d'objets étiquetés, avec les FGE $A(x)$ et $B(x)$, alors la somme $A(x) + B(x)$ peut clairement être interprétée comme la FGE de $\mathcal{A} + \mathcal{B}$, la réunion disjointe des classes $\mathcal{A}$ et $\mathcal{B}$ (voyez-vous pourquoi ?). Par contre, interpréter le produit $A(x) \cdot B(x)$ est moins évident.

Pour rappel, si $a_n := n![x^n]A(x)$ (le nombre d'éléments de taille n dans $\mathcal{A}$) et $b_n := n![x^n]B(x)$ (le nombre d'éléments de taille n dans $\mathcal{B}$), alors $A(x) \cdot B(x)$ est la FGE de la convolution binomiale de $(a_n)_{nN}$ et $(b_n)_{nN}$:

$$n![x^n]A(x) \cdot B(x) = \sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}\,.$$

On interprète ceci de la manière suivante. Pour chaque paire d'objets $\boxed{1\,2\,3\,\cdots\,k}$ dans $\mathcal{A}$ et $\boxed{1\,2\,3\,\cdots\,n-k}$ dans $\mathcal{B}$, on obtient plusieurs objets étiquetés en "concaténant" les deux objets :

$$\boxed{1\,2\,3\,\cdots\,k}\;|\;\boxed{1\,2\,3\,\cdots\,n-k}$$

puis en réétiquetant pour que chaque étiquette de 1 jusque n apparaisse, en préservant l'ordre des étiquettes dans chaque objet. Le réétiquetage peut être fait de $\binom{n}{k}$ manières car cela revient à choisir l'ensemble des k étiquettes données à la partie "gauche" de l'objet résultant.

Par exemple, si $E(x)$ est la FGE de la classe des ensembles non vides, alors $E^2(x)$ est la FGE de la classe

$$\{\{1\}|\{2\},\ \{1\}|\{2,3\},\ \{2\}|\{1,3\},\ \{3\}|\{1,2\},\ \{1,2\}|\{3\},\ \{1,3\}|\{2\},\ \{2,3\}|\{1\},\ \ldots\}$$

des bipartitions (partitions en deux classes non vides) ordonnées. Par analogie, $E^3(x)$ est la FGE de la classe des tripartitions ordonnées, etc… La classe qui nous intéresse est la classe de toutes les partitions ordonnées, dont la FGE peut s'écrire :

$$\underbrace{1}_{\substack{\text{partition}\\ \text{vide}}} + \underbrace{E(x)}_{\substack{\text{partition}\\ \text{en 1 classe}}} + \underbrace{E^2(x)}_{\substack{\text{partition}\\ \text{en 2 classes}}} + \underbrace{E^3(x)}_{\substack{\text{partition}\\ \text{en 3 classes}}} + \ldots = \frac{1}{1-E(x)} = \frac{1}{1-(\mathrm{e}^x-1)} = \frac{1}{2-\mathrm{e}^x}\,.$$

Donc la FGE de la suite $(b_n)_{n\in\mathbb{N}}$ des nombres de Bell ordonnés est

$$B(x) = \frac{1}{2-\mathrm{e}^x}\,.$$

4.4.2 Formule asymptotique pour les nombres de Bell ordonnés

Considérons maintenant la fonction *complexe*

$$B(z) = \frac{1}{2-e^z}\,.$$

Quelles sont les propriétés de cette fonction ?

(i) $B(z)$ est holomorphe sur $\mathbb{C}\backslash\{z\in\mathbb{C} \mid e^z = 2\} = \mathbb{C}\backslash\{z\in\mathbb{C} \mid z = \ln 2 + 2k\pi\cdot i\}$ où $k\in\mathbb{Z}$.

(ii) En ordre de distance par rapport à l'origine, la première singularité de $B(z)$ (la plus proche de 0) est $\ln 2$, la deuxième est $\ln 2 \pm 2\pi\cdot i$ (à une distance de $\sqrt{(\ln 2)^2 + (2\pi)^2} = 6,321\ldots$).

La fonction $B(z)$ est holomorphe (ou analytique) sur un anneau $A := \{z \in \mathcal{C} \mid 0 < |z - \ln 2| < 2\pi\}$ centré en $\ln 2$. Par conséquent, elle peut être développée en série de Laurent autour de $\ln 2$:

$$B(z) = \sum_{n=-\infty}^{+\infty} a_n (z - \ln 2)^n = \underbrace{\sum_{n=-\infty}^{-1} a_n (z - \ln 2)^n}_{\text{partie principale}} + \underbrace{\sum_{n=0}^{\infty} a_n (z - \ln 2)^n}_{\text{partie analytique}} .$$

Montrons :

$$\begin{aligned} a_{-1} &= -\frac{1}{2} \\ a_{-2} &= a_{-3} = \ldots = 0 . \end{aligned}$$

Par la formule de Cauchy, nous avons, pour tout $n \in \mathbb{Z}$:

$$a_n = \frac{1}{2\pi i} \int_{C(\ln 2, \varepsilon)} B(z)(z - \ln 2)^{-n-1} \mathrm{d}z$$

où $C(\ln 2, \varepsilon)$ désigne un cercle de centre $\ln 2$ et rayon $0 < \varepsilon < 2\pi$ parcouru une fois, dans le sens positif. En posant $w = z - \ln 2$, nous avons :

$$a_n = \frac{1}{2\pi i} \int_{C(0,\epsilon)} B(w + \ln 2) w^{-n-1} \mathrm{d}w .$$

Or

$$\begin{aligned} B(w + \ln 2) &= \frac{1}{2 - e^{w + \ln 2}} = \frac{1}{2 - 2 \cdot e^w} \\ &= \frac{1}{2 - 2\left(1 + w + \frac{w^2}{2!} + \frac{w^3}{3!} + \ldots\right)} \\ &= \frac{1}{-2w\left(1 + \frac{w}{2!} + \frac{w^2}{3!} + \ldots\right)} \\ &= -\frac{1}{2} \cdot \frac{1}{w \cdot f(w)} \qquad \text{où } f(w) \text{ est holomorphe sur } \mathbb{C} \end{aligned}$$

Donc

$$a_n = \frac{1}{2\pi i} \int_{C(0,\epsilon)} \underbrace{-\frac{1}{2} \cdot \frac{1}{f(w)}}_{\substack{\text{fonction holomorphe} \\ \text{en 0, et qui vaut} \\ -\frac{1}{2} \text{ quand } w = 0}} w^{-n-2} \mathrm{d}w .$$

En conlusion, a_n n'est autre que le coefficient coefficient de w^{n+1} dans la série de Taylor de la fonction holomorphe $F(w) := -\frac{1}{2}\frac{1}{f(w)}$ autour de 0. Nous obtenons donc : $a_{-2} = a_{-3} = \ldots$ car $F(w)$, étant holomorphe, a une partie principale nulle ; $a_{-1} = F(0)$ car a_{-1} est le coefficient de $w^{-1+1} = w^0$, c'est-à-dire le terme indépendant, dans la série de Taylor de $F(w)$.

On peut donc écrire :

$$B(z) = \underbrace{\frac{-\frac{1}{2}}{z - \ln 2}}_{\text{partie principale}} + \underbrace{\left(B(z) - \frac{-\frac{1}{2}}{z - \ln 2}\right)}_{=:\hat{B}(z) \text{ partie analytique}}$$

avec $\hat{B}(z)$ holomorphe sur un disque ouvert de centre 0 et de rayon $|\ln 2 \pm 2\pi i| = \sqrt{(\ln 2)^2 + (2\pi)^2} > 6,321$.

Développons $\hat{B}(z)$ en série de Taylor autour de 0 :

$$\hat{B}(z) = \sum_{n=0}^{\infty} \hat{b}_n \, z^n \, .$$

Cette série de puissances converge absolument au moins pour $|z| \leqslant 6,321$. En particulier, la série réelle

$$\sum_{n=0}^{\infty} |\hat{b}_n| (6,321)^n$$

converge, ce qui implique en particulier (chaque terme étant au plus 1)

$$|\hat{b}_n| (6,321)^n \leqslant 1$$

et donc

$$|\hat{b}_n| \leqslant (0,16)^n \, .$$

Développer la partie principale de $B(z)$ est facile :

$$\begin{aligned} \frac{-\frac{1}{2}}{z - \ln 2} &= \frac{\frac{1}{2\ln 2}}{1 - \frac{z}{\ln 2}} \\ &= \frac{1}{2\ln 2} \left(1 + \frac{z}{\ln 2} + \left(\frac{z}{\ln 2} \right)^2 + \dots \right) \\ &= \sum_{n=0}^{\infty} \frac{1}{2} \left(\frac{1}{\ln 2} \right)^{n+1} z^n \end{aligned}$$

Etant donné que le coefficient de z^n dans $B(z)$ est $\frac{b_n}{n!}$ (par définition) et que le coefficient de z^n dans $B(z) - \hat{B}(z)$ est réel, le coefficient de z^n dans $\hat{B}(z)$ l'est nécessairement aussi ($\hat{b}_n \in \mathbb{R}$).

Nous sommes près du but :

$$\begin{aligned} b_n &= n! [z^n] B(z) \\ &= n! \left(\frac{1}{2} \left(\frac{1}{\ln 2} \right)^{n+1} + \hat{b}_n \right) \\ &= \frac{n!}{2} (\log_2 \mathrm{e})^{n+1} + n! \, \hat{b}_n \, . \end{aligned}$$

Ci-dessus, on a utilisé $\frac{1}{\ln 2} = \frac{1}{\log_e 2} = \log_2 e$ (remarque : $\lg e = 1,44\ldots$).

Finalement, on trouve l'encadrement suivant :

$$\frac{n!}{2} (\log_2 \mathrm{e})^{n+1} - n! \, (0,16)^n \leqslant b_n \leqslant \frac{n!}{2} (\log_2 \mathrm{e})^{n+1} + n! \, (0,16)^n \, ,$$

ce qui donne le résultat suivant.

Théorème 4.16. *Le n-ème nombre de Bell ordonné b_n satisfait*

$$b_n \sim \frac{n!}{2} (\log_2 \mathrm{e})^{n+1} \, .$$

Exemple 4.17. Comme nous pouvons le voir sur le tableau ci-dessous, le résultat que nous avons obtenu est *extrêmement* bon.

n	1	2	3	5	10
b_n	1	3	13	541	10224763
$\frac{n!}{2}(\log_2 \mathrm{e})^{n+1}$	$\approx 1,04$	$\approx 3,002$	$\approx 12,997$	$\approx 541,002$	≈ 10224763

4.5 Exercices

Exercice 4.1. (Examen janvier 2011.) Que valent les limites suivantes ?

a) $\lim\limits_{n\to\infty} \dfrac{n!\,n!\,n!}{(3n)!}$

b) $\lim\limits_{n\to\infty} \sum\limits_{k=3n}^{7n} \dfrac{1}{k}$

c) $\lim\limits_{n\to\infty} \dfrac{F_{2n}}{(1+\varphi)^n}$

Exercice 4.2. (Examen août 2011.) Que valent les limites suivantes ?

a) $\lim\limits_{n\to\infty} \sum\limits_{k=5n}^{8n} \dfrac{1}{k}$

b) $\lim\limits_{n\to\infty} \sqrt[n]{\dfrac{(n!)^2}{(2n)!}}$

c) $\lim\limits_{n\to\infty} \dfrac{F_n}{\varphi^n}$

Exercice 4.3. (Examen janvier 2011.) Soit $f(n) = \binom{n}{\lceil n/4 \rceil}$ pour $n \in \mathbb{N}$. Pour quels $c > 0$ a-t-on $f(n) = O(c^n)$?

Chapitre 5

Introduction à la théorie de l'information

5.1 Entropie

L'*entropie* (binaire) d'une distribution de probabilités discrète $p = \{p_i\}_{i\in[n]} = \{p_1, \ldots, p_n\}$ est définie par (pour rappel, $\lg x = \log_2 x$)

$$H(p) = -\sum_{i\in[n]} p_i \lg p_i = \sum_{i\in[n]} p_i \lg \frac{1}{p_i} .$$

Observons que $H(p)$ est la moyenne pondérée des quantités $\lg \frac{1}{p_i} \geqslant 0$. Donc en particulier $H(p) \geqslant 0$.

L'entropie d'une distribution de probabilités est une mesure de l'incertitude associée à cette distribution. Une distribution dont l'incertitude est "grande" a une grande entropie, et une distribution dont l'incertitude est "petite" a une petite entropie.

Exemple 5.1. Pour $n = 2$, considérons la distribution $p = \{p_1, p_2\}$. Considérons des distributions d'incertitude de plus en plus petite.

1. Si $p_1 = p_2 = \frac{1}{2}$ (incertitude maximum), on a
$$H(p) = -\frac{1}{2}\lg\left(\frac{1}{2}\right) - \frac{1}{2}\lg\left(\frac{1}{2}\right) = 1$$
2. Si $p_1 = \frac{1}{4}$ et $p_2 = \frac{3}{4}$, on a
$$H(p) = -\frac{1}{4}\lg\left(\frac{1}{4}\right) - \frac{3}{4}\lg\left(\frac{3}{4}\right) = \lg 4 - \frac{3}{4}\lg 3 \approx 0,811$$
3. Si $p_1 = 0$ et $p_2 = 1$ (incertitude nulle), on a
$$H(p) = -0\lg 0 - 1\lg 1 = 0 + 0 = 0$$
(On pose $-p_i \lg p_i = 0$ si $p_i = 0$.)

Lemme 5.2. *Pour toute distribution $p = \{p_i\}_{i\in[n]}$,*

$$0 \leqslant H(p) \leqslant \lg n .$$

De plus, $H(p) = 0$ si et seulement si p est entièrement concentrée sur un indice $j \in [n]$, c'est-à-dire $p_i = 1$ si $i = j$ et $p_i = 0$ si $i \neq j$; $H(p) = \lg n$ si et seulement si p est uniforme, c'est-à-dire $p_i = 1/n$ pour tout i.

Démonstration. Premièrement,

$$H(p) = \sum_i p_i \underbrace{\lg \frac{1}{p_i}}_{\geqslant 0} \geqslant 0$$

avec égalité si et seulement si $p_i \lg \frac{1}{p_i} = 0$ pour tout i, donc si et seulement si $p_i \in \{0, 1\}$ pour tout i, ce qui signifie (p étant une distribution de probabilité) que p est concentrée sur un indice $j \in [n]$.

Deuxièmement, en utilisant $\lg x = \log_2 x = \frac{\ln x}{\ln 2}$ puis $\ln x \leqslant x - 1$ (pour $x > 0$), on a

$$\begin{aligned}
\lg n - H(p) &= \overbrace{\sum_i p_i}^{=1} \lg n + \sum_i p_i \lg p_i \\
&= -\sum_i p_i \lg \frac{1}{np_i} \\
&= \frac{-1}{\ln 2} \sum_i p_i \ln \frac{1}{np_i} \\
&\geqslant \frac{-1}{\ln 2} \sum_i p_i \left(\frac{1}{np_i} - 1 \right) \\
&= \frac{-1}{\ln 2} \left(\sum_i \frac{1}{n} - \sum_i p_i \right) \\
&= 0 \,.
\end{aligned}$$

De plus, comme $\ln x = x - 1$ ssi $x = 1$, on a égalité ssi $\frac{1}{np_i} = 1$ pour tout i, c'est-à-dire $p_i = \frac{1}{n}$ pour tout i. □

5.2 Application : compression de données

5.2.1 Théorème de Shannon

Soient Σ un alphabet fini et $M \in \Sigma^*$ un mot (*un texte*) sur Σ. Notre but est de donner une réponse satisfaisante à la question suivante, en utilisant l'entropie :

> *Comment encoder chaque symbole $x \in \Sigma$ par un mot binaire $C(x) \in \{0, 1\}^*$ de sorte à ce que la taille de l'encodage résultant de M soit minimum ?*

Une précision imporante : l'encodage doit être *sans préfixe*, c'est-à-dire que le code $C(x)$ d'un symbole ne peut être un préfixe du code $C(y)$ d'un autre symbole. Ainsi, il y a une et une seule façon de décoder l'encodage du texte M.

Exemple 5.3. $\Sigma = \{i, m, p, s\}$, $M =$ mississipi. Si on pose

$$\begin{aligned}
C(i) &= 1 \\
C(m) &= 010 \\
C(p) &= 011 \\
C(s) &= 00
\end{aligned}$$

alors l'encodage de M est

$$C(M) = 010100001000010111 \,.$$

Remarquons que la longueur de $C(M)$ est

$$|C(M)| = 4 \cdot 1 + 4 \cdot 2 + 1 \cdot 3 + 1 \cdot 3 = 18 \,.$$

On peut toujours écrire la longueur de $C(M)$ comme le nombre de symboles de M fois le nombre moyen de bits par symbole dans l'encodage de M. En d'autres termes, si on note p_x la fréquence relative du symbole x dans M, on a

$$\begin{aligned} |C(M)| &= \sum_{x \in \Sigma} \underbrace{(\text{\#occurences de } x \text{ dans } M)}_{=|M|p_x} \cdot |C(x)| \\ &= |M| \cdot \sum_{x \in \Sigma} p_x |C(x)| \\ &= |M| \cdot (\text{\#moyen de bits par symbole}) \end{aligned}$$

Il s'avère que le nombre moyen de bits par symbole d'un code sans préfixe est *toujours* au moins l'entropie de la distribution $p = \{p_x\}_{x \in \Sigma}$! C'est une limite fondamentale mise en évidence par Claude Shannon, le père de la théorie de l'information. Nous donnerons plus tard la démonstration de ce théorème.

Théorème 5.4 (Shannon, 1948). *Pour tout mot $M \in \Sigma^*$ et tout code sans préfixe $C : \Sigma \to \{0,1\}^*$,*

$$\sum_{x \in \Sigma} p_x |C(x)| \geqslant H(p)$$

où $p = \{p_x\}_{x \in \Sigma}$ est la distribution des fréquences des symboles $x \in \Sigma$ dans M.

Ceci peut également s'écrire

$$|C(M)| \geqslant |M| \cdot H(p) \,.$$

Dans l'exemple 5.3, on a

$$H(p) \approx 1,72$$

et donc, par le théorème de Shannon,

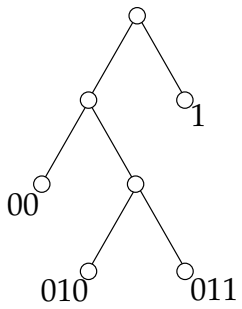
$$|C(M)| \geqslant 10 \cdot 1,72 = 17,2$$

ce qui montre que 18 (la taille de notre encodage) est la taille minimum que l'on peut avoir.

5.2.2 Inégalité de Kraft

Toute code binaire sans préfixe peut se représenter dans un arbre binaire enraciné dont les feuilles sont les mots du code. Pour reformer les mots, le principe est simple : en partant de la racine, on choisit à chaque étape un des deux fils du noeud courant. Si le fils gauche est choisi, on écrit un "0". Sinon, le fils droit est choisi, et on écrit un "1". Ainsi de suite jusqu'à atteindre une feuille.

Exemple 5.5 (Suite exemple 5.3)**.** L'arbre binaire enraciné correspondant au code sans préfixe $C(i) = 1$, $C(m) = 010$, $C(p) = 011$ et $C(s) = 00$ est :



Observons que

$$2^{-|C(i)|} + 2^{-|C(m)|} + 2^{-|C(p)|} + 2^{-|C(s)|} = \frac{1}{2} + \frac{1}{8} + \frac{1}{8} + \frac{1}{4} = 1\,.$$

Le résultat suivant généralise cette observation et joue un rôle primordial dans la démonstration du théorème de Shannon (voir ci-dessous).

Théorème 5.6 (Kraft, 1949). *Pour tout code sans préfixe $C : \Sigma \to \{0,1\}^*$, on a*

$$\sum_{x \in \Sigma} 2^{-|C(x)|} \leqslant 1\,.$$

Démonstration. En rajoutant des symboles dans Σ et en étendant C, on peut supposer que dans l'arbre correspondant à C *tout* sommet interne a exactement deux fils. (On dit que le code C est *complet*.) Montrons que dans ce cas

$$\sum_{x \in \Sigma} 2^{-|C(x)|} = 1 \tag{5.1}$$

par induction sur $|\Sigma|$, le nombre de symboles à encoder. Pour le cas de base, $|\Sigma| = 2$ et

$$\sum_{x \in \Sigma} 2^{-|C(x)|} = \frac{1}{2} + \frac{1}{2} = 1\,.$$

Supposons maintenant que $|\Sigma| > 2$ et que (5.1) est satisfaite pour tout alphabet plus petit que Σ. Soient $y, z \in \Sigma$ des symboles dont les feuilles correspondantes sont les deux fils d'un même noeud interne de l'arbre de C. Alors on peut supposer que les mots de code de y et z sont de la forme $C(y) = w0$ et $C(z) = w1$ pour un mot binaire w. En retirant y et z de Σ et en les remplaçant par un nouveau symbole t dont le mot de code est w, on obtient un nouveau code complet $C' : \Sigma' \to \{0,1\}^*$ sur l'alphabet $\Sigma' := (\Sigma \setminus \{y,z\}) \cup \{t\}$, qui comporte un symbole de moins que Σ. Par l'hypothèse d'induction,

$$\begin{aligned}
1 &= \sum_{x \in \Sigma'} 2^{-|C'(x)|} \\
&= \sum_{\substack{x \in \Sigma' \\ x \neq t}} 2^{-|C'(x)|} + 2^{-|C'(t)|} \\
&= \sum_{\substack{x \in \Sigma \\ x \neq y,z}} 2^{-|C(x)|} + 2^{-|C(y)|} + 2^{-|C(z)|} \\
&= \sum_{x \in \Sigma} 2^{-|C(x)|}\,.
\end{aligned}$$

□

Théorème 5.7. *Si une longueur $\ell(x) \in \mathbb{N}$ est donnée pour chaque symbole $x \in \Sigma$ de telle sorte que*

$$\sum_{x \in \Sigma} 2^{\ell(x)} \leqslant 1 \,,$$

il existe un code sans préfixe $C : \Sigma \to \{0,1\}^*$ qui a les longueurs données, c'est-à-dire

$$\forall x \in \Sigma : |C(x)| = \ell(x) \,.$$

Démonstration. Supposons $\Sigma = \{x_1, x_2, \ldots, x_n\}$ avec $\ell(x_1) \leqslant \ell(x_2) \leqslant \ldots \leqslant \ell(x_n)$. Nous construisons un code C par l'intermédiaire d'un arbre binaire enraciné. Dans l'arbre binaire enraciné infini, associons à chaque x_j le premier sommet disponible de profondeur $\ell(x_j)$. Il reste à démontrer qu'il existe toujours un sommet disponible à la profondeur $\ell(x_j)$ dans l'arbre.

On sait

$$\sum_{i<j} 2^{-\ell(x_i)} < 1 \iff \sum_{i<j} 2^{-\ell(x_j)} \cdot 2^{\ell(x_j)-\ell(x_i)} < 1$$

ce qui peut s'écrire

$$\sum_{i<j} 2^{\ell(x_j)-\ell(x_i)} < 2^{\ell(x_j)} \,.$$

Le membre de droite est le nombre total de sommets de profondeur $\ell(x_j)$ dans l'arbre. Etant donné que $\ell(x_j) \geqslant \ell(x_i)$ pour $i < j$, chaque terme du membre de gauche peut s'interpéter comme le nombre de sommets de profondeur $\ell(x_j)$ interdits par le choix d'un sommet de profondeur $\ell(x_i)$ pour x_i. L'inégalité signifie qu'il reste un sommet disponible de profondeur $\ell(x_j)$ pour x_j. □

Nous pouvons maintenant prouver le théorème de Shannon.

Démonstration du théorème 5.4. Posons $n := |\Sigma|$. Pour simplifier les notations, notons $p_i := p_{x_i}$ la fréquence relative du $i$ème symbole de Σ (pour $i \in [n]$). Le nombre moyen de bits par symbole du code C est au moins le nombre minimum moyen de bits par symbole d'un code binaire sans préfixe, qui par l'inégalité de Kraft et sa réciproque (théorèmes 5.6 et 5.7) peut s'exprimer comme

$$\min \left\{ \sum_{i=1}^{n} p_i \ell_i \mid \sum_{i=1}^{n} 2^{-\ell_i} \leqslant 1,\ \ell_i \in \mathbb{N}\ \forall i \in [n] \right\} \,. \tag{5.2}$$

Ce nombre est à son tour au moins

$$\min \left\{ \sum_{i=1}^{n} p_i \ell_i \mid \sum_{i=1}^{n} 2^{-\ell_i} = 1,\ \ell_i \in \mathbb{R}\ \forall i \in [n] \right\} \,. \tag{5.3}$$

Pour résoudre ce problème d'optimisation sous contrainte, cherchons les points critiques du lagrangien

$$F(\ell; \lambda) := \sum_{i=1}^{n} p_i \ell_i + \lambda \left(\sum_{i=1}^{n} 2^{-\ell_i} - 1 \right) \,.$$

Le calcul des dérivées partielles donne :

$$\frac{\partial F}{\partial \ell_i} = p_i + \lambda \frac{\partial}{\partial \ell_i}(2^{-\ell_i}) = p_i - \lambda \ln 2 \cdot 2^{-\ell_i} \quad \text{pour } i \in [n]$$
$$\frac{\partial F}{\partial \lambda} = \sum_{i=1}^{n} 2^{-\ell_i} - 1 \,.$$

On obtient donc

$$\begin{cases} p_i - \lambda \cdot \ln 2 \cdot 2^{-\ell_i} = 0 \quad \text{pour } i \in [n] \\ \sum_{i=1}^{n} 2^{-\ell_i} - 1 = 0 \end{cases} \iff \begin{cases} \ell_i = -\lg\left(\frac{p_i}{\lambda \ln 2}\right) \quad \text{pour } i \in [n] \\ \sum_{i=1}^{n} \frac{p_i}{\lambda \ln 2} = 1 \end{cases}$$

Etant donné que $\sum_{i=1}^{n} p_i = 1$, on obtient $\lambda \ln 2 = 1$ et $\ell_i = -\lg p_i$ pour $i \in [n]$. Le lagrangien du problème d'optimisation (5.3) n'admet donc qu'un seul point critique. On peut vérifier que ce point donne bien le minimum recherché en (5.3), qui n'est autre que l'entropie de $p = \{p_i\}_{i \in [n]}$ car au point critique,

$$\sum_{i=1}^{n} p_i \ell_i = -\sum_{i=1}^{n} p_i \lg p_i = H(p) \,.$$

□

Dans la preuve du théorème de Shannon, on voit que le minimum est atteint en prenant $\ell_i = -\lg p_i = \lg \frac{1}{p_i}$. Ces longueurs n'étant pas forcément entières, cela donne envie de les arrondir vers le haut et poser $\ell_i := \lceil -\lg p_i \rceil$. Ces nouvelles longueurs ℓ_i sont entières et satisfont l'inégalité de Kraft. De plus,

$$\begin{aligned} \sum_{i=1}^{n} p_i \ell_i &= \sum_{i=1}^{n} p_i \lceil -\lg p_i \rceil \\ &\leqslant \sum_{i=1}^{n} p_i (-\lg p_i + 1) \\ &= H(p) + \sum_{i=1}^{n} p_i \\ &= H(p) + 1 \end{aligned}$$

On voit donc qu'on peut toujours trouver un code binaire sans préfixe C tel que $|C(x_i)| = \lceil -\lg p_i \rceil$ qui est "presque optimal" au sens que

$$H(p) \leqslant \#\text{moyen de bits par symbole} \leqslant H(p) + 1 \,.$$

Nous verrons comment obtenir un tel code à la section suivante.

5.3 Arbres de Huffman

On construit itérativement un arbre comme suit :

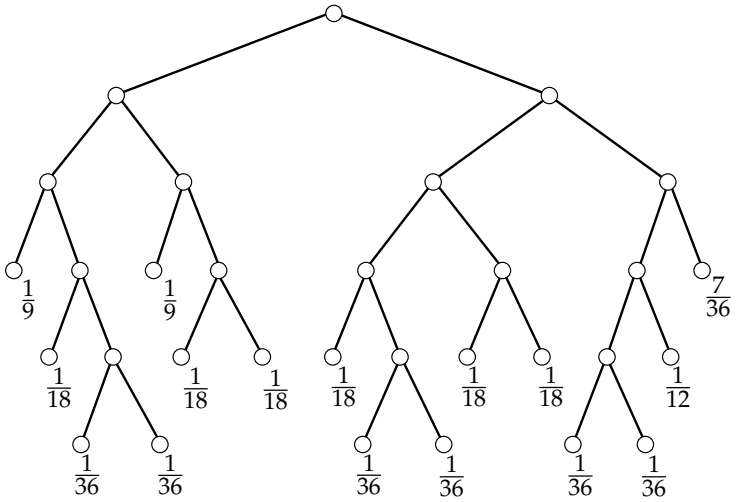
- Initialement, créer une racine par symbole dans Σ, pondéré par sa probabilité respective.
- Tant qu'il existe au moins deux racines :

– Prendre les deux racines x, y de plus petite probabilité ;
– Ajouter une nouvelle racine z, qui devient le père de x et y, et poser $p_z = p_x + p_y$.

L'arbre résultant s'appelle *arbre de Huffman*. Le code binaire correspondant s'appelle *code de Huffman*.

Exemple 5.8. Voici un arbre de Huffman pour la distribution

$$\{p_i\}_{i\in[16]} = \left\{ \frac{7}{36}, \frac{4}{36}, \frac{4}{36}, \frac{3}{36}, \frac{2}{36}, \frac{2}{36}, \frac{2}{36}, \frac{2}{36}, \frac{2}{36}, \frac{2}{36}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36}, \frac{1}{36} \right\} .$$



On peut démontrer le résultat suivant en montrant que l'algorithme de Huffman trouve un code binaire tel que le nombre moyen de bits par symbole est minimum, c'est-à-dire résout le problème d'optimisation (5.2).

Théorème 5.9. *Si C_{Huff} est un code de Huffman pour le mot $M \in \Sigma^*$ et $p = \{p_x\}_{x\in\Sigma}$ est la distribution associée à M, alors*

$$\#\textit{moyen de bits par symbole} = \sum_{x\in\Sigma} p_x \, |C_{\text{Huff}}(x)| \leqslant H(p) + 1 \, .$$

Ceci peut s'ecrire

$$|C_{\text{Huff}}(M)| \leq |M| \cdot (H(p) + 1) \, .$$