الجمهوريـة الجزائـريـة الديمقراطيـة الشعبيـة
République Algérienne Démocratique et Populaire
وزارة التعليـم العالـي والبحـث العلمـي
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

N° Réf : ....

Centre Universitaire
Abd Elhafid Boussouf Mila

Institut des Mathématiques et Informatique Département de Mathématiques et Informatique

Mémoire préparé En vue de l'obtention du diplôme de Master

En: Mathématiques

Spécialité : Mathématiques appliquées

Fonctions génératrices en sciences appliquées

Préparé par :

- Saliha Atemani
- Manal Kikah

Soutenue devant le jury

Halim Yacine	M.C. A	C. U. Abdelhafid Boussouf, Mila	Président
Bazeniar Abdelghafour	M.C. B	C. U. Abdelhafid Boussouf, Mila	Rapporteur
Boufelgha Ibrahim	M.A. A	C. U. Abdelhafid Boussouf, Mila	Examinateur

Année universitaire: 2022/2023

Remerciements

Avant tout nous remercions *ALLAH* le tout puissant et Miséricordieux qui m'a donné la force, la réussite et la patience d'accomplr ce modeste travail.

Nous sommes très sensibles à l'intérêt qu'ont bien voulu porter à ce travail Monsieur *Abdelghafour Bazeniar*, maître de conférences au centre universitaire Abdelhafid Boussouf de Mila.

Nous tenons à le remercier pour m'avoir fait l'honneur d'être rapporteur de ce mémoire.

Nous tenons à remercier également, Monsieur *Yacine Halim* maître de conférence au centre universitaire.

Abdelhafid Boussouf de Mila et Monsieur *Ibrahim Boufelgha* maître de conférence au centre universitaire Abdelhafid Boussouf de Mila pour m'avoir fait l'honneur d'être membres de notre jury.

Nous remercions également l'ensemble du personnel du département de mathématiques et informatique de centre universitaire.

Dédicace

Du profond de mon cœur, je dédie ce travail a tous ceux me sont chers.

A celle qui le paradis sous ses pieds. A celle qui s'est privée et donnée, et attendu avec patience les fruits de sa bonne éducation.

A ma chère mère

A celui qui fait mon affiliation avec me rend fier. A celui qui changé la nuit en jour pour m'assurer les bonnes conditions.

A mon cher père

A mes chères frères Abdanour et Ayoub, mes sœurs WAssila , Amina et hadjar, les fils de mon sœurs Mouhamd Akram et Sadjed.

A tous les membres de ma famille.

A tous mes amis Amal, Ghada, Wissal , Rania et Chaima, En particulier Manal.

Merci !

Saliha. A

Dédicace

Je dédie ce mémoire à :

Ma mère, qui à ouvré pour ma réussite, de par son amour, son soutien, tous les sacrifices consentis et ses précieux conseils, pour tout son assistance est sa présence dans ma vie

Mon père, qui être fier et trouver ici le résultat de longues années de sacrifices et de privation pour m'aider à avancer dans la vie.

Mes frères Amine, Mouhssin, Bassam, Khiro et Mes sœurs Rania, Djahida, HAkima, Madiha

Tous mes amis Amel, Ghada a ceux qui m'ont accompagné pendant cec cinq années de douleur et de joie Saliha

Merci.

Manal. K

TABLE DES MATIÈRES

INTRODUCTION

La théorie de la combinatoire est une branche des mathématiques qui consiste à énumérer, trouver des bijections, chercher des interprétations combinatoires et verifier des identités et des propriétés sous certains conditions spécifiques.

Les premiers pas des fonctions génératrices sont du à Moivre, Stirling et Euler en 18 siècle. Aujourd'hui, cet outil puissant de la combinatoire apparaissent dans des domaines d'études très variés et qui sert à résoudre des problèmes liés au comptage en analyse combinatoire, à l'analyse de la dynamique de populations en biologie, à l'analyse des algorithmes en informatique et les moments en statistique.

Les fonctions génératrices permettent d'obtenir une formule explicite de certains suites connus par ces relations de récurrences. Elles permettent aussi de prouver des identités combinatoire passant par les fonctions rationnelles [17]. Il existe de nombreuses techniques est méthodes pour manipuler les fonctions génératrices et ça dépend de la nature du problème et les objectifs à visés. Dans ce travail, d'abord, on va présenter au lecteur un aperçus général sur les fonctions génératrices accompagné par des exemples explicatifs. Ensuite, on va étudier l'application de ces fonctions dans les différents disciplines de la science appliquée.

Ce mémoire présente une étude théorique et pratique sur les fonctions génératrices, organisé en trois chapitre.

Dans le premier chapitre, on a estimé que presenter les fonctions génératrices comme un outil de résolution est assez efficace pour mieux commencer avec cette théorie. Pour cela, un problème classique à savoir le problème de *billet chanceux* sera exposé et étudié rigoureusement. Ensuite, on introduit toute un formalise sur les définitions et les concepts de base des séries formelles, des fonctions génératrices ordinaires et exponentielles avec des relations de récurrence.

Le deuxième chapitre sera consacré aux notions et différents techniques de bases sur les opérations possibles des fonctions génératrices. Ce qui enrichit ce chapitre, est le faite d'essayer d'écrire un petit catalogue de certaine fonctions génératrices connues dans la littérature associées à des suites réels.

Le dernier chapitre est le fruit des deux chapitres précédent, car on va voir comment appliquer ce qu'on a initié et ça dans certaines domaines des sciences appliquées. De manière choisie, l'application sera en statistiques, en combinatoire en théorie des graphes et en informatique.

CHAPITRE 1

PRÉLIMINAIRES

1.1 Motivation

En URSS, au début des années 70 du siècle dernier, un problème mathématique appelé probléme de billet chanceux est apparu. Le scientifique A. Kirillov (mathématicien russe) a initié ce problème : un passager du bus devait acheter un billet qui est composé de 6 chiffres. Pour lui récompenser d'un prix, les organisateurs ont déterminé le gagnant si la somme des trois premiers numéros est égale à la somme des trois derniers numéros. Pour touts les billets vendus, la personne détenant le billet dont le numéro correspond remporte le prix[11] .

Illustration

– Si le billet porte le numéro 123060 :

$$1 + 2 + 3 = 6$$

$$0 + 6 + 0 = 6$$

alors, le billet est chanceux.

– Si le billet porte le numéro 245780 :

$$2 + 4 + 5 = 11$$

$$7 + 8 + 0 = 15$$

alors, le billet n'est pas chanceux.

Exemple 1.1.1 *(Exemple pratique)*
Dans touts les spectacles du Sirk Ammar, tous ceux qui voulaient entrer devaient acheter un billet à la caisse, le billet se compose de quatre numéros, et tous ceux qui ont obtenu un billet chanceux sont entrés gratuitement. Aidons le caissier à compter le nombre de tickets chanceux (on dit que le billet est chanceux si la somme des deux premier nombres égale à la somme des deux derniers nombres).

Solution : Touts les billets chanceux sont compris entre 0000 et 9999. La démarche à suivre consiste à diviser les numéros en deux parties. La somme des numéros de la première partie est comprise entre 0 et 18. Pour calculer le nombre de billet chanceux, il suffit de calculer a_n puis de calculer a_n^2 comme suit :

n : La somme des nombres.

a_n : Le nombre de façon d'écrire la somme.

1. **D'abord un nombre à un chiffre :** en utilisant la somme de n pour chaque $0 \leq n \leq 9$, il existe un nombre à un chiffre sur la somme de n

chiffres. Il est composé de la somme d'un nombre :

$$\begin{cases} n = 0 \Rightarrow a_0 = 1 \\ n = 1 \Rightarrow a_1 = 1 \\ \vdots \\ n = 9 \Rightarrow a_9 = 1. \end{cases}$$

Nous additionnons les nombres qui composent les termes à un chiffre, alors la solution s'écrit en tant que suite polynômial :

$$A_1(X) = X^0 + X^1 + X^2 + ... + X^9,$$

avec, X^n représente l'indéterminé qui correspond au nombre de chiffres à un chiffre.

2. Ensuite un nombre à deux chiffres :

$$\begin{cases} n = 0 \Rightarrow a_0 = 1; n = 1 \Rightarrow a_1 = 2; n = 2 \Rightarrow a_2 = 3 \\ \vdots \\ n = 9 \Rightarrow a_9 = 10; n = 10 \Rightarrow a_{10} = 9; n = 11 \Rightarrow a_{11} = 8 \\ \vdots \\ n = 18 \Rightarrow a_{18} = 1. \end{cases}$$

Bref, a_n représente le nombre de façons de répartir n en deux. Par exemple, pour $n = 9$ on a $a_9 = 10$.

Les possibilités	1	2	3	4	5	6	7	8	9	10
n=9	(0 9)	(9 0)	(8 1)	(1 8)	(7 2)	(2 7)	(4 5)	(5 4)	(3 6)	(6 3)

Alors, la suite des n peut s'écrire de manière polynômial comme suit,

$$A_2(X) = X^0 + 2X^1 + ... + 10X^9 + 9X^{11} + ... + X^{18}.$$

Consequence : $A_2(X) = (A_1(X))^2$.

Preuve de la Consequence : Le produit de deux monômes X^k et X^m contribue au coefficient du monôme X^n dans le polynôme $(A_1(X))^2$ si et seulement si : $n = k + m$. Par conséquent, le coefficient de X^n dans $(A_1(X))^2$ est exactement le nombre de façons de représenter n comme une somme $n = k + m$.

Le problème du billet chanceux est quasiment résolu, il ne reste plus qu' à calculer le polynôme A_2 puis trouver la somme des carrés de ses coefficients avec le polynôme A_2.

Considérons le "polynôme de Laurent"$A_2(\frac{1}{X})$ dans les variables :

$$A_2\left(\frac{1}{X}\right) = a_0 + \frac{a_1}{X} + \frac{a_2}{X^2} + ... + \frac{a_{18}}{X^{18}}.$$

La solution consiste à éliminer l'indéterminé X, en appuyant sur le polynôme de Laurent :

$$\begin{aligned} A_2(X)A_2\left(\frac{1}{X}\right) &= a_0^2 + a_1^2 + a_2^2 + ... + a_{18}^2, \\ &= 1^2 + 2^2 + 3^2 + ... + 10^2 + ... + 1^2, \\ &= 670. \end{aligned}$$

Donc le nombre des billets chanceux est de 670.

Conclusion : Enfin, on a arriver à construire des formules fermées et finies. Ces formules aident à établir des polynômes qui contribuent à traduire le problème en opérations des fonctions génératrices (voir chapitre 2).

Dans le reste de ce chapitre, le lecteur peut se trouver face aux certaines phrases et même des petits paragraphes qui lui paraître familiar (sites spécialités). Dans certains cas on a préféré de recopié certaines informations ou définitions qui sont très connus en literature. Certes, cela n'empêche pas les efforts fournis pour la compréhension.

1.2 Séries formelles

En mathématiques, les séries formelles sont un outil qui permet d'utiliser l'arsenal analytique des séries entières sans tenir compte de la notion de convergence. Ces séries sont également très utiles pour décrire de façon concise des suites et pour trouver des formules pour des suites définies par récurrence via ce que l'on appelle les fonctions génératrice. Considérons un anneau commutatif $\mathbb{K}$. On définit l'anneau des séries formelles sur $\mathbb{K}$ de l'indéterminée X, noté $\mathbb{K}[[X]]$, comme un ensemble des éléments de cet anneau qui sera écrit de façon unique comme une somme infinie de la forme $\sum_{n\geq 0} a_n X^n$. Où les coefficients a_n sont des éléments de $\mathbb{K}$.

Définition 1.2.1 *Soit* $\mathbb{K} = \mathbb{R}$ ($\mathbb{Q}$ *où*$\mathbb{C}$) *un anneau commutatif (unifère). L'anneau* $\mathbb{K}[[X]]$ *des séries formelles sur* $\mathbb{K}$ *en une indéterminée* X *est le groupe abélien* $(\mathbb{K}^N, +)$ *des suites à valeurs dans* $\mathbb{K}$, *muni d'une certaine loi interne de multiplication.*

Définition 1.2.2 *Soit* $(a_0, a_1, a_2, \ldots)$ *une suite arbitraire (infinie) de nombre. La fonction génératrice (série génératrice) de cette suite est l'expression de la forme*

$$P(X) = \sum_{n=0}^{\infty} a_n X^n, \tag{1.1}$$

a_n *s'appelle les coefficients de la série dans* $\mathbb{K}$. $a_n X^n$ *s'appelle le monôme de degré* n *et* a_n *est son coefficient.*

Définition 1.2.3 *(Ordre d'une série formelle)*
Soit $P(X) = \sum\limits_{n\geq 0} a_n X^n$ *une série formelle. Son ordre* $Ord(S)$ *est un entier qui n'est défini que si* $P \neq 0$. *C'est le plus petit* n *tel que* $a_n \neq 0$. *Si* $\mathbb{K}$ *est intègre alors l'anneau*

$\mathbb{K}[[X]]$ *l'est aussi, et* $Ord(PQ) = Ord(P) + Ord(Q)$ *pour* P *et* Q *non nulles dans cet anneau.*

Exemple 1.2.1 – *La série formelle* $X^3 + \sum\limits_{i\geq 4} 2^i X^i$ *à pour ordre* 3.

– *La série formelle* $X^3 + \sum_{i\geq 1} 2X^i$ *à pour ordre* 1.

Définition 1.2.4 *Une série formelle* $a_0 + a_1X + a_2X^2 + \cdots$. *Où* a_n *est fini et non nuls est appelé polynôme formel.*

Définition 1.2.5 *(Degré d'un polynôme)*

Le degré d'un polynôme $\sum_{i=0}^{n} a_iX^i$ *est le plus grand entier* i *tel que* a_i *est différent de* 0.

Exemple 1.2.2 – *Le polynome* $X^2 + 2X + 1$ *à pour degré* 2.

– *Le polynome* $X^5 + 4X^3 + 1$ *à pour degré* 5.

Remarque 1.2.1 *Soit* $\mathbb{K}[X]$ *l'ensemble des polynômes à coefficients dans* $\mathbb{K}$ *est un sous ensemble de* $\mathbb{K}[X]$.

Remarque 1.2.2 *Du coté algébrique, l'ensemble des séries formelles forme un espace vectoriel sur la dimension* $\mathbb{K}$. *La multiplication transforme cet espace en algèbre noté* $\mathbb{K}[[X]]$.

1.3 Les types des fonctions génératrices

1.3.1 Les fonctions génératrices ordinaires (FGO)

La fonction génératrice ordinaire est une fonction mathématique qui permet de représenter une suite d'objets mathématiques en une fonction unique. Cette fonction est souvent utilisée en combinatoire et en théorie des nombres pour étudier des propriétés des suites d'objets [5, 6, 13, 17].

Définition 1.3.1 *[1]. La fonction génératrice ordinaire (FGO) de la suite :*

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

est définie par :

$$G(X) = \sum_{n=0}^{\infty} a_n X^n. \tag{1.2}$$

Exemple 1.3.1 – *La FGO de* $(1, 1, 1, ...)$ *est :*

$$G(X) = \sum_{n=0}^{\infty} X^n = 1 + X + X^2 + X^3 + ... = \frac{1}{1-X}.$$

– *La FGO de la suite* (2^n) *est :*

$$G(X) = \sum_{n=0}^{\infty} 2^n X^n = 1 + 2X + 2^2X^2 + ... + 2^nX^n = \frac{1}{1-2X}.$$

Les résultats aux dessous, nous permettre d'obtenir la FGO d'une suite obtenue en faisant des opérations simple (addition, multiplication,...etc) sur une ou plusieurs suites dont on connaît leurs fonctions génératrices ordinaires.

Proposition 1.3.1 *[1] 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 :*

1. $A(X) + B(X)$ *est la FGO de* $(a_n + b_n)_{n\in\mathbb{N}}$.
2. $XA(X)$ *est la FGO de* $(0, a_0, a_1, a_2, ..., a_{n-1}, ...)$.
3. $A'(X)$ *est la FGO de*$(0, a_1, 2a_2, 3a_3, ..., (n+1)a_{n+1}, ...)$.
4. $A(X)B(X)$ *est la FGO de* $(a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_2, ...)$.
5. $(1-X)A(X)$ *est la FGO de*$(a_0, a_1 - a_0, a_2 - a_1, \ldots, a_n - a_{n-1}, \ldots)$.
6. $\int_0^X A(X)dX$ *est la FGO de* $(0, a_0, \frac{a_1}{2}, \frac{a_2}{3}, \ldots, \frac{a_{n-1}}{n}, \ldots)$.
7. $\frac{A(X) - a_0}{X}$ *est la FGO de* $(a_1, a_2, a_3, ..., a_{n+1}, ...)$.
8. $\frac{A(X)}{1-X}$ *est la FGO de* $(a_0, a_0 + a_1, a_0 + a_1 + a_2 + \ldots, \sum_{k=0}^{n} a_k, \ldots)$.

Les relations de recurrences

On peut résoudre des relations de récurrence linéaire à coefficients constants homogènes ou non homogènes en utilisant les FGO.

Théorème 1.3.1 *[1] Soit la suite $(G_n)_{n\in\mathbb{N}}$ définie par la relation de récurrence suivante :*

$$\begin{cases} G_n = pG_{n-1} + qG_{n-2}, n \geq 2, \\ G_0 = \alpha, G_1 = \beta. \end{cases} \tag{1.3}$$

Avec $p, q \in \mathbb{R}_+^*$ et $\alpha, \beta \in \mathbb{C}$. Alors la fonction génératrice associée à $(G_n)_{n\in\mathbb{N}}$ est donnée par :

$$G(X) = \frac{\alpha + (\beta - p\alpha)X}{1 - pX - qX^2}. \tag{1.4}$$

Preuve. On a :

$$\begin{aligned} G(X) &= \sum_{n=0}^{\infty} G_n X^n, \\ &= G_0 + G_1 X + \sum_{n=2}^{\infty} G_n X^n, \\ &= \alpha + \beta X + \sum_{n=2}^{\infty} (pG_{n-1} + qG_{n-2}) X^n, \end{aligned}$$

$$
\begin{aligned}
&= \alpha + \beta X + pX \sum_{n=2}^{\infty} G_{n-1} X^{n-1} + qX^2 \sum_{n=2}^{\infty} G_{n-2} X^{n-2}, \\
&= \alpha + \beta X + pX \sum_{n=1}^{\infty} G_n X^n + qX^2 \sum_{n=0}^{\infty} G_n X^n, \\
&= \alpha + \beta X + pX \left(\sum_{n=0}^{\infty} G_n X^n - \alpha \right) + qX^2 \sum_{n=0}^{\infty} G_n X^n, \\
&= \alpha + (\beta - p\alpha)X + pXG(X) + qX^2 G(X).
\end{aligned}
$$

Alors :

$$G(X)(1 - pX - qX^2) = \alpha + (\beta - \alpha p)X,$$

d'oú :

$$G(X) = \frac{\alpha + (\beta - p\alpha)X}{1 - pX - qX^2}.$$

■

D'après le théorème précédant on déduit les fonctions génératrices suivantes :

1. Pour $\alpha = k, \beta = q = 1, p = k$, nous obtenons la fonction génératrice des nombres de k-Fibonacci :

$$G(X) = \frac{1}{1 - kX - X^2}.$$

2. Pour $\alpha = 0, \beta = 1, p = 3k, q = -2$, nous obtenons la fonction génératrice de nombre de k-Mersenne :

$$G(X) = \frac{1}{1 - 3kX + 2X^2}.$$

3. Pour $\alpha = 2, \beta = p = 3k, q = -2$, nous obtenons la fonction génératrice de nombre de k-Mersenne-Lucas :

$$G(X) = \frac{2 - 3kX}{1 - 3kX + 2X^2}.$$

Pour $k = 1$ dans les relations précédentes on obtient les fonctions génératrices suivantes :

– La fonction génératrice des nombres de Fibonacci est donnée par :

$$G(X) = \frac{1}{1 - X - X^2}.$$

– La fonction génératrice de Mersenne est donnée par :

$$G(X) = \frac{1}{1 - 3X + 2X^2}.$$

– La fonction génératrice de Mersenne-Lucas est donnée par :

$$G(X) = \frac{2 - 3X}{1 - 3X + 2X^2}.$$

Théorème 1.3.2 *[1] Soit la suite $(W_n)_{n\in\mathbb{N}}$ définie par la relation de récurrence suivante :*

$$\begin{cases} W_n = aW_{n-1} + bW_{n-2} + cW_{n-3}, n \geq 3 \\ W_0 = \alpha, W_1 = \beta, W_3 = \gamma. \end{cases} \tag{1.5}$$

Avec $a, b, c \in \mathbb{R}$ et $\alpha, \beta, \gamma \in \mathbb{C}$. Alors la fonction génératrice associée à $(W_n)_{n\in\mathbb{N}}$ est donnée par :

$$G(X) = \frac{\alpha + (\beta - \alpha a)X + (\gamma - \beta a - b\alpha)X^2}{1 - aX - bX^2 - cX^3}. \tag{1.6}$$

Preuve. On a :

$$\begin{aligned}
G(X) &= \sum_{n=0}^{\infty} w_n X^n, \\
&= w_0 + w_1 + w_2 x^2 + \sum_{n=3}^{\infty} (aW_{n-1} + bW_{n-2} + cW_{n-3}) X^n, \\
&= \alpha + \beta X + \gamma X^2 + aX \sum_{n=3}^{\infty} W_{n-1} X^{n-1} + bX^2 + \sum_{n=3}^{\infty} W_{n-2} X^{n-2} + cX^3 + \sum_{n=3}^{\infty} W_{n-3} X^{n-3}, \\
&= \alpha + \beta X + \gamma X^2 + aX \sum_{n=2}^{\infty} W_n X^n + bX^2 + \sum_{n=1}^{\infty} W_n X^n + cX^3 + \sum_{n=0}^{\infty} W_n X^n, \\
&= \alpha + \beta X + \gamma X^2 + aX \left(\sum_{n=0}^{\infty} W_n X^n - \alpha - \beta X \right) + bX^2 \left(\sum_{n=0}^{\infty} W_n X^n - \alpha \right) + cX^3 \sum_{n=0}^{\infty} W_n X^n, \\
&= \alpha + \beta X + \gamma X^2 + aX \sum_{n=0}^{\infty} W_n X^n - \alpha a X - a\beta X^2 + bX^2 \sum_{n=0}^{\infty} W_n X^n - \alpha b X^2 + cX^3 \sum_{n=0}^{\infty} W_n X^n, \\
&= \alpha + \beta X + \gamma X^2 + aXG(X) - \alpha a X - a\beta X^2 + bX^2 G(X) - \alpha b X^2 + cX^3 G(X).
\end{aligned}$$

Alors :

$$G(X)(1 - aX - bX^2 - cX^3) = \alpha + (\beta - a\alpha)X + (\gamma - \beta a - b\alpha)X^2,$$

d'où :

$$G(X) = \frac{\alpha + (\beta - \alpha a)X + (\gamma - \beta a - b\alpha)X^2}{1 - aX - bX^2 - cX^3}.$$

■

D'après le théorème précédant on déduit les fonctions génératrices suivantes :

1. Pour $\alpha = \beta = \gamma = 1$, $a = 0$, $b = c = 1$, nous obtenons la fonction génératrice de la suite $(p_n)_{n\in\mathbb{N}}$:

$$G(X) = \frac{1 + X}{1 - X^2 - X^3}.$$

2. Pour $\alpha = 0$, $\beta = \gamma = 1$, $a = c = 1$, $b = 0$, nous obtenons la fonction génératrice de la suite $(N_n)_{n\in\mathbb{N}}$:

$$G(X) = \frac{X}{1 - X - X^2}.$$

3. Pour $\alpha = 0$, $\beta = \gamma = 1$, $a = b = 1$, $c = 2$, nous obtenons la fonction génératrice de la suite $(J_n)_{n\in\mathbb{N}}$:

$$\frac{X}{1 - X - X^2 - 2X^3}.$$

4. Pour $\alpha = \beta = \gamma = 1$, $a = 0$, $b = 1$, $c = 2$, nous obtenons la fonction génératrice de la suite $(JP_n)_{n\in\mathbb{N}}$:

$$G(X) = \frac{1 + X}{1 - X^2 - 2X^3}.$$

5. Pour $\alpha = 3$, $\beta = 0$, $\gamma = 10$, $a = 0$, $b = c = 1$, nous obtenons la fonction génératrice de la suite $(R_n)_{n\in\mathbb{N}}$:

$$G(X) = \frac{3 - X^2}{1 - X^2 - X^3}.$$

6. Pour $\alpha = 3$, $\beta = 0$, $\gamma = 10$, $a = 0$, $b = 2$, $c = 1$, nous obtenons la fonction génératrice de la suite $(PR_n)_{n\in\mathbb{N}}$:

$$G(X) = \frac{3 - 4X^2}{1 - 2X^2 - X^3}.$$

7. Pour $\alpha = \beta = 0$, $\gamma = 1$, $a = 0$, $b = c = 1$, nous obtenons la fonction génératrice de la suite $(S_n)_{n\in\mathbb{N}}$:

$$G(X) = \frac{X^2}{1 - 2X^2 - X^3}.$$

Théorème 1.3.3 *[1] Soit la suite $(P_n(t))_{n\in\mathbb{N}}$ définie par la relation de récurrence suivante :*

$$\begin{cases} P_n(t) = ptP_{n-1}(t) + qP_{n-2}(t), n \geq 2 \\ P_0(t) = \alpha, P_1(t) = \beta t + \gamma. \end{cases} \tag{1.7}$$

Avec $p, q \in \mathbb{R}$ et $\alpha, \beta, \gamma \in \mathbb{C}$, alors la fonction génératrice associée à $(P_n(X))_{n\in\mathbb{N}}$:

$$G(X) = \frac{\alpha + ((\beta - \alpha p)t + \gamma)X}{1 - pXt - qX^2}. \tag{1.8}$$

Preuve. on a

$$\begin{aligned} G(X) &= \sum_{n=0}^{\infty} GP_n(t)X^n, \\ &= P_0(t) + P_1(t)X + \sum_{n=2}^{\infty} P_n(t)X^n, \\ &= \alpha + (\beta t + \gamma)X + pt\sum_{n=2}^{\infty} P_{n-1}(t)X^n + q\sum_{n=2}^{\infty} P_{n-2}(t)X^n, \\ &= \alpha + (\beta t + \gamma)X + ptX\sum_{n=2}^{\infty} P_{n-1}(t)X^{n-1} + qX^2\sum_{n=0}^{\infty} P_n(t)X^n, \\ &= \alpha + (\beta t + \gamma)X + ptX\left(\sum_{n=0}^{\infty} P_n(t)X^n - \alpha\right) + qX^2\sum_{n=0}^{\infty} P_n(t)X^n, \\ &= \alpha + (\beta t + \gamma)X + ptX\sum_{n=0}^{\infty} P_n(t)X^n - \alpha ptX + qX^2\sum_{n=0}^{\infty} P_n(t)X^n, \\ &= \alpha + ((\beta - \alpha p)t + \gamma)X + ptXG(X) + qX^2G(X). \end{aligned}$$

Alors :

$$G(X)(1 - ptX - qX^2) = \alpha + ((\beta - \alpha p)t + \gamma)X,$$

donc :

$$G(X) = \frac{\alpha + ((\beta - \alpha p)t + \gamma)X}{1 - pXt - qX^2}.$$

■

D'après le théorème précédent nous déduit les fonctions génératrices suivants :

1. Pour $\alpha = \beta = 0,\ \gamma = p = 1,\ q = -1$, nous obtenons la fonction génératrice associée à $(v_n(X))_{n\in\mathbb{N}}$:

$$G(X) = \frac{X}{1 - tX + X^2}. \tag{1.9}$$

2. Pour $\alpha = 2,\ \beta = 1,\ \gamma = 0,\ p = 1,\ q = -1$, nous obtenons la fonction génératrice associée à $(u_n(X))_{n\in\mathbb{N}}$:

$$G(X) = \frac{2 - tX}{1 - tX + X^2}.$$

3. Pour $\alpha = \beta = 0,\ \gamma = 1,\ p = 2,\ q = 1$, nous obtenons la fonction génératrice associée à $(t_n(X))_{n\in\mathbb{N}}$:

$$G(X) = \frac{X}{1 - 2tX + X^2}.$$

4. Pour $\alpha = 2,\ \beta = \gamma = 0,\ p = 1,\ q = -1$, nous obtenons la fonction génératrice associée à $(s_n(X))_{n\in\mathbb{N}}$:

$$G(X) = \frac{2 - 2tX}{1 - tX + X^2}.$$

5. Pour $\alpha = 1,\ \beta = 1,\ \gamma = 0,\ p = 2,\ q = -1$, la fonction génératrice des polynômes de Tchebychev de la première espèce $(T_n(X))$ est :

$$G(X) = \frac{1 - tX}{1 - 2tX + X^2}.$$

6. Pour $\alpha = 1,\ \beta = 2,\ \delta = 0,\ p = 2,\ q = -1$, la fonction génératrice des polynômes de Tchebychev de la deuxième espèce $(U_n(X))$ est :

$$G(X) = \frac{1}{1 - 2tX + X^2}.$$

7. Pour $\alpha = 1,\ \beta = 2,\ \gamma = -1,\ p = 2,\ q = -1$, la fonction génératrice des polynômes de Tchebychev de la troisième espèce $(V_n(X))$ est :

$$G(X) = \frac{1 - X}{1 - 2tX + X^2}.$$

8. Pour $\alpha = 1,\ \beta = 2,\ \gamma = 1,\ p = 1,\ q = -1$, la fonction génératrice des polynômes de Tchebychev de la quatrième espèce $(W_n(X))$ est :

$$G(X) = \frac{1 + X}{1 - 2tX + X^2}.$$

Deux types de suites

Définition 1.3.2 *[3] : On appelle série alternée, toute série dont le terme général est*

$$u_n = (-1)^n a_n,\ a_n \geq 0, \forall n \in \mathbb{N}.$$

où (a_n) est un suite réelle de signe constant. À un signe près, une série alternée s'écrit donc $\sum(-1)^n a_n$ où (a_n) est une suite à terme positif. Lorsque la suite est à valeurs non nulles, cette définition équivalente à :

$$\forall n \in \mathbb{N} \quad u_n u_{n+1} < 0.$$

Exemple 1.3.2 – *Un exemple classique de série alternée est la série :*

Exemple 1.3.3

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

– *Un exemple du même type est la formule de libiniz*

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

Définition 1.3.3 *Le terme général* (u_n) *de la série harmonique est défini par :*

$$\forall n \in \mathbb{N} \quad u_n = \frac{1}{n}.$$

On appelle $n^{\text{ème}}$ *nombre harmonique (noté classiquement* H_n*) la* $n^{\text{ème}}$ *somme partielle de la série harmonique, qui est donc égal à :*

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}.$$

Définition 1.3.4 *Le terme général* (u_n) *de la série harmonique alternée est définie par :*

$$\forall n \in \mathbb{N} \quad u_n = \frac{(-1)^n}{n}.$$

1.3.2 Les Fonctions génératrices exponentielles(FGE)

La fonction génératrice exponentielle, également appelée fonction génératrice de moments exponentiels, est une fonction qui est souvent utilisée en théorie des probabilités et en statistique pour caractériser les distributions de probabilité exponentielles.

Définition 1.3.5 *[6] La fonction génératrice exponentielle (FGE) de la suite :*

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

est définie par :

$$A(X) = \sum_{n=0}^{\infty} a_n \frac{X^n}{n!}. \tag{1.10}$$

Exemple 1.3.4 *La FGE de* $(1,1,1...) = \left(\binom{n}{k}\right)_{n\in\mathbb{N}}$ *est* $\sum_{n=0}^{\infty} \frac{X^n}{n!} = e^X$.

Proposition 1.3.2 *[6] 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*

1. $A(X)+B(X)$ *est la FGE de* $(a_0+b_0, a_1+b_1, ..., a_n+b_n, ...)$.
2. $XA(X)$ *est la FGE de* $(0, a_0, 2a_1, 3a_2, ..., a_{n+1}, ...)$.
3. $A'(X)$ *est la FGE de* $(a_1, a_2, a_3, a_4, ..., a_{n+1}, ...)$.
4. $A(X)B(X)$ *est la FGE de* $(a_0b_0, a_0b_1+a_1b_0, a_0b_2+2a_1b_1+a_2b_0, ..., \sum\limits_{k=0}^{n} \binom{n}{k} a_k b_{n-k}, ...)$.
5. $A'(X)-A(0)$ *est la FGE de*$(a_1-a_0, a_2-a_1, ..., a_{n+1}-a_n, ...)$.
6. $\int_0^X A(t)dt$ *est la FGE de* $(0, a_0, a_1, a_2, ..., a_{n-1}, ...)$.
7. $\dfrac{A(X)-A(0)}{X}$ *est la FGE de* $(a_1, \frac{a_2}{2}, \frac{a_3}{3}, ..., \frac{a_{n+1}}{n+1}, ...)$.
8. $e^X A(X)$ *est la FGE de* $(a_0, a_0+a_1, a_0+2a_1+a_2, ..., \sum\limits_{k=0}^{n} \binom{n}{k} a_k, ...)$.

Les relations de recurrences

On peut résoudre des relation de récurrence linéaire à coefficients constants homogènes ou non homogènes en utilisant les FGE.

Coefficient t^n	Fonctions génératrice
$F_n(X)$	$\frac{1}{1-Xt-t^2}$
$L_n(X)$	$\frac{2-Xt}{1-Xt-t^2}$
$P_n(X)$	$\frac{t}{1-2Xt-t^2}$
$Q_n(X)$	$\frac{2-2Xt}{1-2Xt-t^2}$
$U_n(X)$	$\frac{1}{1-2Xt+t^2}$
$T_n(X)$	$\frac{1-Xt}{1-2Xt+t^2}$
$J_n(X)$	$\frac{t}{1-t-2Xt}$

1.1-Fonctions génératrice des polynômes.

Généralisations : La FGE de $\left(\binom{n}{k}\right)_{n\in\mathbb{N}}$ est,

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

Exemple 1.3.5 *Soit la relation de récurrnce suivant :*

$$\begin{cases} d_n = nd_{n-1}+(-1)^n \quad n\geq 1.\\ d_0=1 \end{cases}$$

On pose,

$$A(X)=\sum_{n=k}^{\infty}d_n\frac{X_n}{n!}$$

Après le calcule on obtient,

$$\begin{aligned} A(X) &= XA(X)+e^{-X}\\ &= \frac{1}{1-X}e^{-X}\\ &= \left(\sum_{n\geq 0}X^n\right)\left(\sum_{n\geq 0}(-1)^n\frac{X^n}{n!}\right)\\ &= \sum_{n\geq 0}n!\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right)\frac{X^n}{n!}, \end{aligned}$$

Donc

$$d_n=n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}.$$

CHAPITRE 2

OPÉRATIONS SUR LES SÉRIES GÉNÉRATRICES

Les fonctions génératrices sont des outils puissants en théorie des nombres et en combinatoire pour étudier les propriétés de différentes suites de nombres, les opérations sur les fonctions génératrices permettent de combiner deux ou plusieurs suites de nombres pour en créer de nouvelles. Voici quelques-unes des opérations les plus courantes sur ces fonctions : addition, soustraction, convolutions, dérivation, Intégration,...etc. Ces opérations peuvent être utilisées pour résoudre de nombreux problèmes, tels que le calcul les nombres de partitions, les nombres de Catalan, les nombres de Fibonacci,... etc [5, 8, 11].

2.1 Addition et Soustraction

L'addition et la soustraction des fonctions génératrices peuvent être utiles dans certaines situations, par exemple pour déterminer les coefficients d'une série génératrice qui est la somme ou la différence de deux autres séries génératrices.

Définition 2.1.1 *[11] **(Addition).** Soient $A(X) = \sum_{n\in\mathbb{N}} a_n X^n$ et $B(X) = \sum_{n\in\mathbb{N}} b_n X^n$ deux séries génératrices, alors :*

$$(A+B)(X) = \sum_{n\in\mathbb{N}} (a_n + b_n) X^n. \tag{2.1}$$

Définition 2.1.2 ***(soustraction).** Soient $A(X) = \sum_{n\in\mathbb{N}} a_n X^n$ et $B(X) = \sum_{n\in\mathbb{N}} b_n X^n$ deux séries génératrices, alors :*

$$(A-B)(X) = \sum_{n\in\mathbb{N}} (a_n - b_n) X^n. \tag{2.2}$$

Explication :

$$\begin{aligned}
\langle a_0, a_1, a_2, \ldots\rangle &\longleftrightarrow A(X), \\
\langle b_0, b_1, b_2, \ldots\rangle &\longleftrightarrow B(X), \\
\langle a_0 \pm b_0, a_1 \pm b_1, a_2 \pm b_2, \ldots\rangle &\longleftrightarrow \sum_{n\in\mathbb{N}} (a_n \pm b_n) X^n, \\
&= \sum_{n\in\mathbb{N}} a_n X^n \pm \sum_{n\in\mathbb{N}} b_n X^n, \\
&= A(X) \pm B(X).
\end{aligned}$$

Exemple 2.1.1 *soient $A(X) = \sum_{n\in\mathbb{N}} (-1)^n X^n$, $B(X) = \sum_{n\in\mathbb{N}} X^n$, alors :*

$$(A+B)(X)=\sum_{n\in\mathbb{N}}((-1)^n+1)X^n.$$

.

2.2 Convolutions

Le produit de convolution des fonctions génératrices est une opération importante dans le domaine de la théorie des séries génératrices. Il est utilisé dans de nombreux domaines des mathématiques et de l'informatique, tels que la combinatoire énumérative : permet de déterminer le nombre de structures combinatoires, tels que les permutations, les partitions, les arbres,... etc.

Définition 2.2.1 *[11] **(Produit de convolution).** Soient $A(X)=\sum_{n\in\mathbb{N}}a_nX^n$ et $B(X)=\sum_{n\in\mathbb{N}}b_nX^n$ séries génératrices, alors :*

$$(A\cdot B)(X)=\sum_{n\in\mathbb{N}}\left(\sum_{k=0}^{n}a_kb_{n-k}\right)X^n=\sum_{n\in\mathbb{N}}c_nX^n. \tag{2.3}$$

Explication :

$$\begin{array}{ccc}\langle a_0,a_1,a_2,...\rangle & \longleftrightarrow & A(X),\\ \langle b_0,b_1,b_2,...\rangle & \longleftrightarrow & B(X),\\ \langle c_0,c_1,c_2,...\rangle & \longleftrightarrow & A(X)\cdot B(X).\end{array}$$

avec :

$$c_n=a_0b_n+a_1b_{n-1}+...+a_nb_0.$$

Exemple 2.2.1 *Soient $A(X)=\sum\limits_{n\in\mathbb{N}}X^n=\dfrac{1}{1-X}$, $B(X)=\sum\limits_{n\in\mathbb{N}}nX^n=\dfrac{X}{(1-X)^2}$, alors :*

$$(A\cdot B)(X)=\sum_{n\in\mathbb{N}}\frac{n(n+1)}{2}X^n.$$

2.3 Multiplication

La multiplication par un scalaire est une opération importante dans la manipulation des fonctions génératrices, car elle permet de transformer la fonction génératrice d'un ensemble en une fonction génératrice pour un ensemble similaire avec des propriétés différentes.

Définition 2.3.1 *[11]* ***(Multiplication par un scalaire).*** *Le produit de série génératrice $A(X) = \sum_{n\in\mathbb{N}} a_n X^n$ par le scalaire k, est donnée par :*

$$k \cdot A(X) = k \sum_{n\in\mathbb{N}} a_n X^n = \sum_{n\in\mathbb{N}} k a_n X^n. \tag{2.4}$$

Explication :

$$\begin{aligned}
\langle a_0, a_1, a_2, ...\rangle &\longleftrightarrow A(X), \\
\langle ka_0, ka_1, ka_2, ...\rangle &\longleftrightarrow kA(X), \\
\langle ka_0, ka_1, ka_2, ...\rangle &\longleftrightarrow ka_0 + ka_1 X + ka_2 X^2 + \cdots, \\
&= k(a_0 + a_1 X + a_2 X^2 + \cdots), \\
&= kA(X).
\end{aligned}$$

Propriété : Soient $A(X), B(X) \in \mathbb{K}[[X]]$ et $k, k_1, k_2 \in \mathbb{K}$;

1. $k(A(X).B(X)) = (kA(X))B(X)$.
2. $k(A(X) + B(X)) = kA(X) + kB(X)$.
3. $(k_1 + k_2)A(X) = k_1 A(X) + k_2 A(X)$.
4. $(k_1 k_2)A(X) = k_1(k_2 A(X)) = k_2(k_1 A(X))$.
5. $1A(X) = A(X)$.

Exemple 2.3.1 *soient* $k = 2$, $A(X) = \sum\limits_{n\in\mathbb{N}} X^n$, *alors :*

$$2 \cdot A(X) = 2\sum_{n\in\mathbb{N}} X^n = \sum_{n=0}^{\infty} 2X^n.$$

2.4 Dérivation et Intégration

La dérivation et l'intégration sont des outils importants dans l'utilisation des fonctions génératrices, pour résoudre une variété des problèmes en combinatoire, en probabilités et en théorie des nombres.

Définition 2.4.1 *[5] **(Dérivation).** La dérivée d'une série génératrice* $A(X) = \sum\limits_{n\geq 0} a_n X^n$ *est donné par :*

$$A'(X) = \sum_{n\geq 1} n a_n X^{n-1} = \sum_{n\geq 0}(n+1)a_{n+1}X^n. \tag{2.5}$$

Explication :

$$\begin{aligned}
\langle a_0, a_1, a_2, \ldots\rangle &\longleftrightarrow A(X),\\
\langle a_1, 2a_2, 3a_3, \ldots\rangle &\longleftrightarrow A'(X),\\
\langle a_1, 2a_2, 3a_3, \ldots\rangle &\longleftrightarrow a_1 + 2a_2X + 3a_2X^2 + \cdots,\\
&= \frac{d}{X}(a_0 + a_1X + a_2X^2 + \cdots),\\
&= \frac{d}{X}A(X) = A'(X).
\end{aligned}$$

On utilise aussi la notation dérivation, on a immédiatement :

$$(A(X) + B(X))' = A'(X) + B'(X). \tag{2.6}$$

Et pour tout scalaire k :

$$(k.A(X))' = k.A'(X). \tag{2.7}$$

L'application $A(X) \mapsto A'(X)$ est donc linéaire.

Par récurrence sur m, on obtient :

$$D^m A(X) = \sum_{n\geq 0}(n+1)_m a_{n+m} X^n. \tag{2.8}$$

On a encore la formule :

$$(A(X)B(X))' = A'(X)B(X) + A(X)B'(X). \tag{2.9}$$

Par une vérification simple :

$$\begin{aligned}(A(X)B(X))' &= \sum_{n+m\geq 1}(n+m)a_n b_m X^{n+m-1} \\ &= \sum_{n\geq 1, m\geq 0} n a_n X^{n+m-1} b_m + \sum_{n\geq 0, m\geq 1} m b_n X^{n+m-1} a_n \\ &= A'(X)B(X) + A(X)B'(X).\end{aligned}$$

On a pour tout entier $n \geq 1$:

$$(A(X)^n)' = nA(X)^{n-1}A'(X). \tag{2.10}$$

Exemple 2.4.1 *Soient* $A(X) = \sum_{n\geq 0} X^n = \dfrac{1}{1-X}$ *donc la dérivation* $A(X)$ *par rapport à* X *:*

$$A'(X) = \frac{-1}{(1-X)^2}.$$

Définition 2.4.2 *[5]* ***(Intégration).*** *L'intégrale de la série fomelle* $A(X) = \sum_{n\geq 0} a_n X^n$ *comme suite :*

$$Int(A(X)) = \int A(X)dX = \int \sum_{n\geq 0} a_n X^n dX = \sum_{n\geq 0} \frac{a_n}{n+1} X^{n+1}. \tag{2.11}$$

Explication :

$$\begin{aligned}
\langle a_0, a_1, a_2, \ldots \rangle &\longleftrightarrow A(X), \\
\langle a_0, \frac{a_1}{2}, \frac{a_2}{3}, \ldots \rangle &\longleftrightarrow Int(A(X)), \\
\langle a_0, \frac{a_1}{2}, \frac{a_2}{3}, \ldots \rangle &\longleftrightarrow a_0 X + \frac{a_1}{2} X^2 + \frac{a_2}{3} X^3 + \cdots, \\
&= Int(a_0 + a_1 X + a_2 X^2 + \cdots), \\
&= Int(A(X)) = \int A(X)dX.
\end{aligned}$$

Exemple 2.4.2 *soient* $A(X) = \sum_{n=0}^{\infty} (-1)^n X^n$ *le résultat de l'intégration de A(X) :*

$$Int(A(X)) = \sum_{n=0}^{\infty} \frac{(-1)^n}{n+1} X^{n+1}.$$

2.5 Division

La division est un outil important dans l'utilisation des fonctions génératrices pour résoudre une variété des problèmes en comptage, analye d'algorithme, probabilités et cryptographie.

Définition 2.5.1 *[11] **(Division).** Soient* $A(X) = \sum_{n\in\mathbb{N}} a_n X^n$ *et* $B(X) = \sum_{n\in\mathbb{N}} b_n X^n$ *deux séries génératrices tels que* $B(X) \neq 0$, $B(X)$ *divise* $A(X)$ *si et seulement s'il existe une série génératrice* $\omega(X)$ *telle que :*

$$A(X) = B(X)\omega(X). \tag{2.12}$$

Proposition 2.5.1 *Toute série formelle $A(X) = \sum_{n=0}^{\infty} a_n X^n$ possède un opposé par l'addition qui est :*

$$(-A(X)) = \sum_{n=0}^{\infty}(-a_n)X^n. \tag{2.13}$$

2.6 Séries inversibles

Définition 2.6.1 *[5] On dit que la série $\sum\limits_{n=0}^{\infty} b_n X^n$ est l'inverse de la série $\sum\limits_{n=0}^{\infty} a_n X^n$ si*

$$\left(\sum_{n=0}^{\infty} a_n X^n\right)\left(\sum_{n=0}^{\infty} b_n X^n\right) = 1. \tag{2.14}$$

Exemple 2.6.1 *La série $\sum\limits_{n=0}^{\infty} X^n$ est l'inverse de $1 - X$*

$$\begin{aligned}\left(\sum_{n=0}^{+\infty} X^n\right)(1-X) &= \sum_{n=0}^{+\infty} X^n - \sum_{n=0}^{+\infty} X^{n+1},\\ &= X^0 + \sum_{n=1}^{+\infty} X^n - \sum_{n=1}^{+\infty} X^n,\\ &= 1.\end{aligned}$$

Proposition 2.6.1 *[8] Une série formelle $\sum\limits_{n=1}^{+\infty} a_n X^n$ est inversible si et seulement si $a_0 \neq 0$.*

Exemple 2.6.2 *La série $\sum\limits_{n\in\mathbb{N}} X^n$ est inversible car $a_0 = 1 \neq 0$.*

Preuve. Soient $A(X) = \sum\limits_{n=1}^{+\infty} a_n X^n$ et $B(X) = \sum\limits_{n=1}^{+\infty} b_n X^n$ deux séries formelles(séries génératrices) telle que

$$A(X)B(X) = 1 \tag{2.15}$$

donc nécessairement

$$a_0 b_0 = 1 \quad et \quad \forall n \in \mathbb{N}^*, \sum_{n=0}^{k} a_n b_{k-n} = 0$$

alors le coefficient $a_0 \neq 0$ Réciproquement, supposons que $a_0 \neq 0$, alors le système triangulaire d'équation

$$\begin{cases} a_0b_0 = 0, \\ a_1b_0 + a_0a_1 = 0, \\ \vdots \\ a_nb_0 + a_{n-1}b_1 + \cdots + a_0b_n = 0. \end{cases}$$

a une unique solution. ■

Proposition 2.6.2 *Si $A(X)$ une série inversible, son inverse est unique.*

Preuve. Soit $A(X)$ une série inversible, $B(X)$ et $C(X)$ deux inverses de $A(X)$, alors :

$$\begin{aligned} A(X)B(X) &= A(X)C(X) = 1, \\ C(X)A(X)B(X) &= C(X)1, \\ B(X) &= C(X). \end{aligned}$$

■

2.7 Compositions des fonctions génératrices

Définition 2.7.1 *[5] Soit $A \in \mathbb{K}[[X]]$ telle que $Ord(A) \geq 1$ et $B(X) = \sum_{n\geq 0} b_nX^n \in \mathbb{K}[[X]]$. On appelle composée de B par A et on note $B(A)$ (ou $B \circ A$) à série génératrice $\sum_{n\geq 0} b_nA^n$ on dit que $B \circ A$ est obtenue par substitution de A à X dans B.*

Théorème 2.7.1 *[1] L'application $B \mapsto B \circ A$ de $\mathbb{K}[[X]]$ dans lui-même est un homorphisme de $\mathbb{K}$-algèebre. Ceci veut dire qu'on a les propriétés suivantes de la substitution :*

1− $(B_1 + B_2) \circ A = B_1 \circ A + B_2 \circ A.$

2− $(B_1B_2) \circ A = (B_1 \circ A)(B_2 \circ A)$.

3− $\lambda \circ A = \lambda$.

Proposition 2.7.1 *Soient A, B et S dans $\mathbb{K}[[X]]$ avec $Ord(A) \geq 1, Ord(B) \geq 1$ (et donc $Ord(A \circ B) \geq 1$). Alors*

$$S \circ (B \circ A) = (S \circ B) \circ A.$$

2.8 Combinaison linéaires

Les opérations de combinaison linéaire sont des opérations mathématiques qui impliquent la multiplication et l'addition de termes. Soit E un espace vectoriel sur un corps $\mathbb{K}$.

Définition 2.8.1 *Soient $X_1, X_2, ..., X_n$ des vecteurs de E. La famille $\{X_1, X_2, ..., X_n\}$ est une famille génératrice de l'espace vectoriel si tout vecteur de E est une combinaison linéaire des vecteurs $X_1, X_2, ..., X_n$.*

Ce qui peut s'écrire aussi :

$$\forall V \in E, \quad a_1, a_2, ..., a_n \in \mathbb{K}, \quad V = a_1X_1 + a_2X_2 + \cdots + a_nX_n = \sum_{i=1}^{n} a_iX_i. \tag{2.16}$$

où $a_1, a_2, ..., a_n$ sont des coefficents scalaires et $X_1, X_2, ..., X_n$ sont des variables ou des vecteurs.

Proposition 2.8.1 *1. Si $U = \sum_{i=1}^{n} a_iX_i$ et $V = \sum_{i=1}^{n} b_iX_i$ sont deux vecteurs, leur somme linéaire est donnée par*

$$U + V = (a_1 + b_1)X + (a_2 + b_2)X^2 + \cdots.$$

2. Si $c = 3$ est un scalaire et $V = \sum_{i=1}^{n} b_iX_i$ est un vecteur, leur produit scalaire est *donné par*

$$3V = 3\sum_{i=1}^{n} b_i X_i = 3a_1X + 3a_2X^2 + \cdots + 3a_nX^n.$$

2.9 Fonctions génératrices connues

La fonction génératrice est utilisée pour représenter une suite de nombres sous forme d'une fonction. Voici quelques fonctions génératrices courantes : fonction génératrice ordinaire, fonction génératrice de bell et fonction génératrice de Catalan ...etc.

2.9.1 Fonctions génératrices associées à la suite de Fibonacci

Considérons la suite de Fibonacci définie par [6] :

$$\begin{cases} F_n = F_{n-1} + F_{n-2}, n \geq 2, \\ F_0 = 0, F_1 = 1. \end{cases}$$

Posons :

$$S(F)(X) = G(X) = \sum_{n=0}^{\infty} F_n X^n,$$

$$\begin{aligned} G(X) &= F_0 + F_1X + \sum_{n=2}^{\infty} (F_{n-1} + F_{n-2}) X^n, \\ &= 0 + X + X\left(\sum_{n=0}^{\infty} F_n X^n - F_0\right) + X^2 \sum_{n=2}^{\infty} F_{n-2} X^{n-2}, \\ &= X + XG(X) + X^2G(X). \end{aligned}$$

Donc,

$$G(X) = \frac{X}{1 - X - X^2}.$$

L'équation caractéristique est $1 - X - X^2 = 0$, qui a pour racines simples avec

$\triangle = 5$. Alors

$$X_1 = \frac{-1-\sqrt{5}}{2} \text{ et } X_2 = \frac{-1+\sqrt{5}}{2}.$$

La solution générale est donnée par :

$$F_n = c_1 X_1^n + c_2 X_2^n,$$

avec les conditions initiales ces constantes c_1 et c_2. En résolvant ce système, on obtient :

$$c_1 = \frac{1}{\sqrt{5}} \text{ et } c_2 = \frac{-1}{5}.$$

Donc F_n s'écrire comme suit :

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]. \tag{2.17}$$

2.9.2 Fonctions génératrices associées à la suite de Pell

Considérons la suite de Pell définie par :

$$\begin{cases} P_n = 2P_{n-1} + P_{n-2}, n \geq 2, \\ P_0 = 0, P_1 = 1. \end{cases}$$

Posons :

$$S(P)(X) = G(X) = \sum_{n=0}^{\infty} P_n X^n,$$

alors la fonction génératrice associée à la suite de Pell est donnée par :

$$G(X) \quad = \quad P_0 + P_1 X + \sum_{n\geq 2} P_n X^n,$$

$$\begin{aligned} &= X + \sum_{n\geq 2}(2P_{n-1} + P_{n-2})X^n, \\ &= X + 2X\left(\sum_{n\geq 0} P_n X^n - P_0\right) + X^2 \sum_{n\geq 0} P_n X^n, \\ &= X + 2XG(X) + X^2 G(X). \end{aligned}$$

Donc,

$$G(X) = \frac{X}{1 - 2X - X^2}. \tag{2.18}$$

On utilise la même démarche appliquée pour la suite de Fibonacci.
Donc la solution générale de la suite de Pell avec $X_1 = -1 - \sqrt{2}$, $X_2 = -1 + \sqrt{2}$ et $c_1 = \frac{-1}{\sqrt{2}}$, $c_2 = \frac{1}{\sqrt{2}}$, s'écrit comme suit :

$$P_n = \frac{1}{2\sqrt{2}}\left[\left(1 + \sqrt{2}\right)^n - \left(1 - \sqrt{2}\right)^n\right]. \tag{2.19}$$

2.9.3 La fonction génératrice des nombres de Catalan

La suite de Catalan $(C_n)_{n\geq 0}$ apparaît dans de nombreux problèmes de dénombrements. Nous allons déterminer la relation de récurrence satisfaite par $(C_n)_{n\geq 0}$ puis en déduire une expression explicite de C_n. Enfin, nous allons exposer quelques problèmes qui utilisent cette suite.
Lorsque l'on effectue une suite d'opérations arithmétiques contenant les quatre opérations, l'ordre des calculs respect les paires de parenthèses [6, 7], par exemple

$$(4 - 5)((77 + 3)/4)(2 + 7).$$

Si l'on efface tous les symboles d'une telle expression à l'exception des parenthèses, on obtient ce que l'on appelle une structure régulière de parenthèses :

$$()(())().$$

Voici toutes les structures régulières de parenthèses contenant une, deux et trois paires de parenthèses respectivement :

$$()$$
$$()() \qquad (())$$
$$()()() \quad ()(()) \quad (())() \quad (()()) \quad ((())).$$

Définition 2.9.1 [6] *Soit $n \geq 0$ un entier. Le nombre de Catalan C_n est le nombre de structures régulières de parenthèses contenant n paires de parenthèses, en convenant que $C_0 = 1$. On note $G(X) = \sum\limits_{k\geq 0} C_k X^k$ la fonction génératrice ordinaire de la suite des nombres de Catalan.*

En vertu de l'exemple précédent et cette définition,on constate donc que la suite des nombres de Catalan commence ainsi :

$$1, 1, 2, 5, ...$$

Question : Afin de déterminer $G(X)$, Peut-on déterminer une relation de récurrence pour C_k ?

Preuve. (Réponse).

Supposons que nous regroupions les termes de sorte que le dernière multiplication se produise entre X_i et X_{i+1} :

$$(X_0 X_1 \cdots X_i)(X_{i+1} \cdots X_k)$$

Ensuite il y a C_i des manières de regrouper les termes dans la première partie du prouduit, et C_{k-1-i} façons la seconde partie, donc il y a $C_i C_{k-1-i}$ façons de regrouper les reprincipaux termes dans ce cas. En sommant sur i, on obtient la formule suivante pour le nombre total de façons de grouper les $k + 1$ termes :

$$C_k = \sum_{i=0}^{k-1} C_i C_{k-1-i}, \qquad k \geq 1. \tag{2.20}$$

On calcul :

$$\begin{aligned}
C_1 &= C_0C_0 = 1,\\
C_2 &= C_0C_1 + C_1C_0 = 1,\\
C_3 &= C_0C_2 + C_1C_1 + C_2C_0 = 5,\\
C_4 &= C_0C_3 + C_1C_2 + C_2C_1 + C_3C_0 = 14,\\
C_5 &= C_0C_4 + C_1C_3 + C_2C_2 + C_3C_1 + C_4C_0 = 42.
\end{aligned}$$

Utilisant la fonction génératrice de cette suite pour trouver la recurrence de C_k,

$$G(X) = \sum_{k\geq 0} C_k X^k.$$

Pour le résoudre, nous avons besoin du principe des produits des fonctions génératrices. Si $A(X) = \sum_{k\geq 0} a_k X^K$ et $B(X) = \sum_{k\geq 0} b_k X^K$, alors

$$A(X)B(X) = \sum_{k>0} \left(\sum_{i=0}^{k} a_i b_{k-i} \right) X^k.$$

Avec, $c_k = \sum_{i=0}^{k} a_i b_{k-i}$. La suite (c_k) est applée la convolution de la suite (a_k) et (b_k). Ainsi, la fonction génératrice de la convolution de deux suites est le produit des fonctions génératrices des suites. En utilisant ce fait, on trouve que

$$G(X) \;=\; \sum_{k\geq 0} C_k X^k,$$

$$\begin{aligned} &= C_0 + \sum_{k\geq 1}\left(\sum_{i=0}^{k-1} C_i C_{k-1-i}\right) X^k, \\ &= 1 + XG(X)^2. \end{aligned}$$

$\left\{\sum_{i=0}^{k-1} C_i C_{k-1-i}\right\}$ est convolution de C_k avec lui-même. Ainsi,

$$XG(X)^2 - G(X) + 1 = 0,$$

donc,

$$G(X) = \frac{1 \pm \sqrt{1-4X}}{2X}.$$

Une seule de ces fonctions peut être la fonction génératrice de C_k, et elle doit satisfaire

$$\lim_{X\to 0} G(X) = C_0 = 1.$$

Il est facile de vérifier que la fonction correct est

$$G(X) = \frac{1 - \sqrt{1-4X}}{2X}.$$

Nous développons maintenant $G(X)$ en série de "Maclaurin" pour trouver une formule pour C_k. En utilisant le Théorème binomial généralisé,

$$\begin{aligned}
(1-4X)^{1/2} &= \sum_{k\geq 0} \binom{1/2}{k} (-4X)^k, \\
&= \sum_{k\geq 0} \binom{k-3/2}{k} 4^k X^k, \\
&= 1 + \sum_{k\geq 1} \binom{k-3/2}{k} 4^k X^k, \\
&= 1 + 4X \sum_{k\geq 0} \binom{k-1/2}{k+1} 4^k X^k,
\end{aligned}$$

donc

$$G(X) = -2 \sum_{k\geq 0} \binom{k-1/2}{k+1} 4^k X^k,$$

et ainsi,

$$C_k = -2^{2k+1} \binom{k-1/2}{k+1}.$$

Nous pouvons trouver une forme beaucoup plus simple pour C_k. Développement du binôme généralisé coefficient et en multipliant chaque terme du produit par 2, nous calculons que

$$\begin{aligned}
C_k &= \frac{-2^{2k+1}}{(k+1)!} \prod_{i=0}^{k} \left(k - \frac{1}{2} - i\right), \\
&= \frac{-2^{2k}}{(k+1)!} \prod_{i=0}^{k} (2k-1-2i)\,.
\end{aligned}$$

Le produit est constitué de tous les nombres impairs entre $(2k-1)$ et -1, donc

$$\begin{aligned}
C_k &= \frac{2^{2k}}{(k+1)!}\prod_{i=1}^{k}(2i-1)\,,\\
&= \frac{2^{2k}}{(k+1)!}\prod_{i=1}^{k}\left(\frac{(2i-1)(2i)}{2i}\right),\\
&= \frac{1}{k!(k+1)!}\prod_{i=1}^{k}((2i-1)(2i))\,.
\end{aligned}$$

Le produit restant est simplement $(2k)!$, donc

$$C_k = \frac{(2k)!}{k!(k+1)!} = \frac{1}{k+1}\binom{2k}{k}. \tag{2.21}$$

Est appelé le $k^{\text{ème}}$ nombre de Catalan. ■

2.9.4 Fonctions génératrices des nombres de Stirling

Dans la littérature, on trouve deux types des nombres de Stirling à deux concepts mathématiques différents, qui sont les nombres de Stirling de première espèce et les nombres de stirling de deuxième espèce. Pour plus de détails voir [9, 10, 14, 17].

Définition 2.9.2 *$S(n,k)$ ou $s(n,k)$ représente n le nombre de façons différentes de choisir un sous-ensemble de k éléments, sans tenir compte de l'ordre dans lequel les éléments sont choisis. On appelle $S(n,k)$ le nombre de Stirling de deuxième espèce (ou $s(n,k)$ le nombre de Stirling de première espèce).*

Nombre de Stirling de première espèce

Définition 2.9.3 *[7] Les nombres de Stirling de première espèce* $\begin{bmatrix} n \\ k \end{bmatrix}$ *sont une classe de nombres entiers qui représente le nombre de permutations d'un ensemble de n éléments ayant exactement k cycles disjoints, ils comptent le nombre de façons de diviser un ensemble de n éléments en k cycles distincts.*

Définition 2.9.4 *[14] Les nombres de Stirling de première espèce* ***signés s(n,k)*** *sont les coefficients du développement de la factorielle décroissante* $(X)^{\underline{n}}$*, c'est-à-dire,*

$$(X)_n = X(X-1)(X-2)...(X-n+1) = \sum_{k=0}^{n} s(n,k)X^k. \tag{2.22}$$

$(X)_0 = 1$ *car il s'agit d'un produit vide.*

Définition 2.9.5 *Les nombres de Stirling de première espèce* ***non signés*** $\mid s(n,k) \mid$ *(valeurs absolues des précédents) sont les coeffcients du développement de la factorielle croissante* $(X)^{\overline{n}}$*, c'est-à-dire que ;*

$$(X)_n = X(X+1)(X+2)...(X+n-1) = \sum_{k=0}^{n} \mid s(n,k) \mid X^k. \tag{2.23}$$

$$X^{\overline{0}} = X^{\underline{0}} = 1.$$

N.B : Il est évident que l'on a pour tout $n \in \mathbb{N}$:

$$(-X)^{\underline{n}} = (-1)^n X^{\overline{n}}. \tag{2.24}$$

Exemple 2.9.1 *On a,*

$$(X)^{\underline{3}} = X(X-1)(X-2) = X^3 - 3X^2 + 2X,$$

d'où,

$$s(3,0) = 0, s(3,1) = 2, s(3,2) = -3, s(3,3) = 1.$$

Proposition 2.9.1 *Pour tous $n, k \in \mathbb{N}$, avec $k \leq n$, le signe du nombre entier $s(n,k)$ est $(-1)^{n+k}$.*

Preuve. Soit $n \in \mathbb{N}$. En substituant dans (2.22) x par $-x$, on obtient

$$(-X)^{\underline{n}} = \sum_{k=0}^{n} s(n,k)(-X)^k,$$

c'est-à-dire

$$(-1)^n X^{\overline{n}} = \sum_{k=0}^{n} (-1)^k s(n,k) X^k,$$

d'où

$$X^{\overline{n}} = \sum_{k=0}^{n} (-1)^{k+n} s(n,k) X^k.$$

Comme les coefficients du polynôme X^n sont de toute évidence tous positifs, on en déduit que $(-1)^{n+k} s(n,k) \geq 0$, $\forall n, k \in \mathbb{N}$, avec $k \leq n$. Autrement dit, le signe de tout nombre $s(n,k)$ est $(-1)^{n+k}$. Ce qui achève cette démonstration.

■

Théorème 2.9.1 *Pour tout $k \in \mathbb{N}$, on a*

$$\sum_{n=k}^{\infty} s(n,k) \frac{X^n}{n!} = \frac{\log^k(1+X)}{k!}. \tag{2.25}$$

Preuve. On détermine de deux façons différentes le développement (formel) de la fonction $f(1+X) = (1+X)^y$, en série de Taylor en y. D'une part, d'après la formule du binôme généralisée, on a

$$\begin{aligned}
(1+X)^y &= 1 + yX + \frac{y(y-1)}{2!}X^2 + + \frac{y(y-1)(y-2)}{3!}X^3 + \cdots, \\
&= \sum_{n=0}^{\infty} y^{\underline{n}} \frac{X^n}{n!}, \\
&= \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} S(n,k) y^k \right) \frac{X^n}{n!}, \\
&= \sum_{n=0}^{\infty} \sum_{k=0}^{n} S(n,k) \frac{y^k X^n}{n!}.
\end{aligned}$$

Soit

$$(1+X)^y = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} s(n,k) \frac{X^n}{n!} \right) y^k, \tag{2.26}$$

d'autre part, d'après le développement de Taylor de la fonction exponentielle, on a

$$(1+X)^y = \exp\{y \log(1+X)\} = \frac{(y\log(1+X))^k}{k!} = \frac{\log^k(1+X)}{k!} y^k, \tag{2.27}$$

l'identification des deux formules (2.25) et (2.26) entraîne (d'après l'unicité du développement de Taylor) que l'on a pour tout $k \in \mathbb{N}$

$$\sum_{n=k}^{\infty} s(n,k) \frac{x^n}{n!} = \frac{\log^k(1+X)}{k!}. \tag{2.28}$$

Le théorème est démontrée. ■

Nombre de Stirling de deuxième espèce

Définition 2.9.6 *[2] Nombres de Stirling de deuxième espèce* $\left\{ \begin{matrix} n \\ k \end{matrix} \right\}$, *notées* $S(n,k)$ *sont des nombres de façons de partitionner un ensemble de* n *éléments en* k *sous-*

ensembles non vides et non ordonnés. On peut également dire que les nombres de Stirling de deuxième espèce mesurent le nombre de façons de diviser un ensemble de n élément en k blocs.

Définition 2.9.7 *[14] Les nombres de Stirling de deuxième espèce sont, par définition les nombres réels $S(n,k)(n,k \in \mathbb{N}, k \leq n)$ qui figurent dans le développement de X^n comme combinaison linéaire des polynômes $X^{\underline{k}}$ $(0 \leq k \leq n)$. On a précisément pour tout $n \in \mathbb{N}$,*

$$\sum_{k=0}^{\infty} S(n,k) X^{\underline{k}}.$$

Exemple 2.9.2

$$(X)^3 = X(X-1)(X-2) + 3X(X-1) + X = X^{\underline{1}} + 3X^{\underline{2}} + X^{\underline{3}},$$

d'où

$$S(3,0) = 0, S(3,1) = 1, S(3,2) = 2 et S(3,3) = 1.$$

Proposition 2.9.2 *Pour tout $n \in \mathbb{N}$, on a*

1. $S(n,0) = 0, \quad S(n,1) = S(n,n) = 1.$
2. $S(n,2) = 2^{n-1} - 1.$
3. $S(n,n-1) = \dfrac{n(n-1)}{2} = \dbinom{n}{k}.$

La série génératrice exponentielle des nombres de Stirling de seconde espèce

Dans le premiere chapitre, nous avons donné les notions nécessaires concernant les fonctions génératrices exponentielles. Plusieurs suites réelles importantes possèdent une série génératrice exponentielle élémentaire. Ceci est le cas de la suite des nombres de Stirling $(S(n,k))_{n \geq k}$ pour $k \in \mathbb{N}$ fixé (i.e, les suites verticales du triangle).

Théorème 2.9.2 *pour tout* $k \in \mathbb{N}^*$*, on a*

$$\sum_{n\geq k} S(n,k)\frac{X^n}{n!} = \frac{(e^X-1)^k}{k!}.$$

Preuve.

Soit $k \in \mathbb{N}$. En utilisant la formule du $S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i \begin{pmatrix} n \\ k \end{pmatrix}(k-i)^n$.

$$\begin{aligned}
\sum_{n\geq k} S(n,k)\frac{X^n}{n!} &= \sum_{n=0}^{\infty} S(n,k)\frac{X^n}{n!}, \\
&= \sum_{n=0}^{\infty}\left\{\frac{1}{k!}\sum_{i=0}^{k}(-1)^i\begin{pmatrix} k \\ i \end{pmatrix}(k-i)^n\right\}\frac{X^n}{n!}, \\
&= \frac{1}{k!}\sum_{n=0}^{\infty}\sum_{i=0}^{k}\left((-1)^i\begin{pmatrix} k \\ i \end{pmatrix}(k-i)^n\frac{X^n}{n!}\right), \\
&= \frac{1}{k!}\sum_{i=0}^{k}\sum_{n=0}^{\infty}\left((-1)^i\begin{pmatrix} k \\ i \end{pmatrix}(k-i)^n\frac{X^n}{n!}\right), \\
&= \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\begin{pmatrix} k \\ i \end{pmatrix}\sum_{n=0}^{\infty}\frac{(X(k-i))^n}{n!}, \\
&= \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\begin{pmatrix} k \\ i \end{pmatrix}e^{(k-i)X}, \\
&= \frac{1}{k!}\sum_{i=0}^{k}\begin{pmatrix} k \\ i \end{pmatrix}(-1)^i(e^X)^{k-i}, \\
&= \frac{(e^X-1)^k}{k!}.
\end{aligned}$$

■

La série génératrice ordinaire des nombres de Stirling de seconde espèce

Dans le premiere chapitre, nous avons donné les notions nécessaires concernant les fonctions génératrices ordinaires. Plusieurs importantes suites réelles possèdent des séries génératrices ordinaires élémentaires et c'est justement le cas de la suite des nombres de Stirling $(S(n,k))_{n\geq k}$ pour $k \in \mathbb{N}$ fixé (i.e, les suites verticales du triangle dressé).

Théorème 2.9.3 *Pour tout $k \in \mathbb{N}$, on a*

$$\sum_{n\geq k} S(n,k)X^n = \frac{X^k}{(1-X)(1-2X)...(1-kX)}. \tag{2.29}$$

Preuve. Soit $k \in \mathbb{N}$. En utilisant la formule du $S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i \begin{pmatrix} k \\ i \end{pmatrix} (k-i)^n$.

$$\begin{aligned}
\sum_{n\geq k} S(n,k)X^n &= \sum_{n=0}^{+\infty} S(n,k)X^n, \\
&= \sum_{n=0}^{+\infty} \left\{ \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \begin{pmatrix} k \\ i \end{pmatrix} (k-i)^n \right\} X^n, \\
&= \sum_{n=0}^{+\infty} \sum_{i=0}^{k} \frac{1}{k!} (-1)^i \begin{pmatrix} k \\ i \end{pmatrix} ((k-i)X)^n, \\
&= \sum_{i=0}^{k} \sum_{n=0}^{+\infty} \frac{1}{k!} (-1)^i \begin{pmatrix} k \\ i \end{pmatrix} ((k-i)X)^n, \\
&= \sum_{i=0}^{k} \left\{ \frac{1}{k!} (-1)^i \begin{pmatrix} k \\ i \end{pmatrix} \sum_{n=0}^{+\infty} ((k-i)X)^n \right\}, \\
&= \sum_{i=0}^{k} \frac{(-1)^i}{i!(k-i)!} \cdot \frac{1}{1-(k-i)X},
\end{aligned}$$

$$\sum_{n\geq k} S(n,k)X^n = \sum_{i=0}^{k} \frac{(-1)^{k-i}}{i!(k-i)!} \cdot \frac{1}{1-iX}.$$

Ainsi, la série $\sum_{n\geq k} S(n,k)X^n$ est une somme finie de fonctions rationnelles, c'est donc une fonction rationnelle qui s'écrit (par réduction à un même dénominateur commun) sous la forme,

$$\sum_{n\geq k} S(n,k)X^n = \frac{p_k(X)}{(1-X)(1-2X)\cdots(1-kX)}. \tag{2.30}$$

où p_k est un polynôme de $\mathbb{Q}[X]$, de degré$\leq k$. Mais puisque lorsque X est au voisinage de 0 on a d'une part

$$\sum_{n\geq k} S(n,k)X^n \sim_0 S(k,k)X^k = X^k,$$

et d'autre part

$$\sum_{n\geq k} S(n,k)X^n \sim_0 p_k(X),$$

il en résulte que $p_k(X) \sim_0 X^k$ ce qui entraîne, du fait que p_k est un polynôme de de $degr \leq k$, que $p_k(X) = X^k$. D'où l'identité recherchée,

$$\sum_{n\geq k} S(n,k)X^n = \frac{X^k}{(1-X)(1-2X)...(1-kX)}.$$

■

2.9.5 La fonction génératrice des partitions

Combien y a-t-il de façon de placer k boules identique dans n urnes identiques sans qu'aucune urnes ne soit vide ? Pour répondre à cette question, nous allons introduire une autre suite de nombres qui va en même temps nous permettre de répondre au problème suivant. Il s'agit du nombre de partition. Il faut faire ici attention de ne pas confondre cette notion de partition avec les partitions d'un ensemble. Dans cette section ce sont les partitions d'un entier qui nous intéresse.

Nous allons définir la solution à ce problème comme étant $p(k, n)$ On appelle ce nombre, le nombre de partition, il n'est pas possible de trouver une formule explicite pour calculer la valeur de $p(k, n)$ (du moins, aucune formule réellement pratique). Remarquez que la solution de notre problème est en fait équivalente par le principe de la bijection à la question de savoir combien y a-t-il de façon d'écrire le nombre k comme une somme de n termes positifs et non nul, si l'ordre des termes n'est pas importante. Ceci nous amène à faire une définition supplémentaire. Nous définirons donc $p(n)$ comme étant [2] :

$$p(n) = \sum_{k=1}^{n} p(n, k). \tag{2.31}$$

Définition 2.9.8 *La valeur de $p(n)$ représente le nombre de façon d'écrire un entier k comme une somme d'entiers positifs non nul.*

Exemple 2.9.3 *Combien y a-t-il de façon de décomposer le nombre 4 comme une somme d'entier positif (n > 0) ? En d'autres termes déterminer $p(4, k)$ et $p(n)$, pour $k = 1, 2, 3, 4$?*

La solution : *On a*

$$\begin{array}{rcll} p(4,1) & = & 1 & (4 = 4), \\ p(4,2) & = & 2 & (2+2=4, 3+1=4), \\ p(4,3) & = & 1 & (2+1+1=4), \\ p(4,4) & = & 1 & (1+1+1+1=4). \end{array}$$

On remarque donc qu'il y a 5 possibilités. Ce nombre correspond à la valeur de $p(5)$.

$$\begin{aligned} p(4) &= p(4,1)+p(4,2)+p(4,3)+p(4,4), \\ &= 1+2+1+1, \\ &= 5. \end{aligned}$$

Définition 2.9.9 *[2] Une partition d'un entier naturel non nul n est une suite décroissante $(m_1, m_2, m_3, \cdots, m_k)$ d'entiers non nuls dont la somme vaut n. le nombre k est la longueur de la partition et les entiers m_n en sont les parts. On représente une telle partition par son diagramme de Ferrers, empilement de i ligne de points (ou de carrés) justifiées à gauche, chaque ligne contenant de haut en bas respectivement etc.*

Exemple 2.9.4 *L'exemple ci-dessous est le diagramme de Ferrers de la partition* $(4, 3, 1, 1)$.

$$\begin{array}{lcccc} m_1 & \bullet & \bullet & \bullet & \bullet \\ m_2 & \bullet & \bullet & \bullet & \\ m_3 & \bullet & & & \\ m4 & \bullet & & & \end{array}$$

Le problème qui se pose maintenant est de trouver la fonction génératrice de $p(n)$. Pour ce faire, écrivons d'abord les fonctions génératrices des nombres des partitions [11].

Soit $P_1(X)$ la fonction génératrice du nombre de partitions de n en parties égales à "k=1", on a :

$$P_1(X) = 1 + X + X^2 + X^3 + \ldots = \frac{1}{1-X}.$$

Le nombre de partitions de n en parties égales à 2 sont un pour n pair et 0 pour les impairs, donc :

$$P_2(X) = 1 + X^2 + X^4 + X^6 + \ldots = \frac{1}{1-X^2}.$$

Ainsi, le nombre de partitions de n en parties n'excédant pas 2 est décrit par la fonction génératrice,

$$P_1(X)P_2(X) = \frac{1}{(1-X)(1-X^2)}.$$

De même, le nombre de partitions de n en parties égales à 3 est décrit par la fonction génératrice $P_3(X) = \dfrac{1}{1-X^3}$, les partitions en parties ne dépassant pas 3 sont énumérées par la fonction génératrice,

$$P_1(X)P_2(X)P_3(X) = \frac{1}{(1-X)(1-X^2)(1-X^3)}.$$

En répétant ce principe, on arrive au théorème suivant.

Théorème 2.9.4 *[4] La fonction génératrice du nombre des partitions de n a la forme :*

$$P(X) = \frac{1}{(1-X)(1-X^2)(1-X^3)\cdots} = \prod_{k=1}^{\infty} \frac{1}{1-X^k}. \tag{2.32}$$

Nous pouvons maintenant établir la fonction génératrice pour $p(n,k)$.

Théorème 2.9.5 *Pour tout $k \in \mathbb{N}$, on a*

$$\sum_{n=k}^{\infty} p(n,k)X^n = X^k \prod_{j=1}^{k} \frac{1}{1-X^j}. \tag{2.33}$$

Preuve. On défini $p(n, \leq k)$ comme étant le nombre de partitions de n en au plus k parties. Simplement $p(n,k) = p(n, \leq k) - p(n, \leq k-1)$. On obtient

$$\sum_{n=k}^{\infty} p(n, \leq k) X^n = \prod_{j=1}^{k} \frac{1}{1-X^j}.$$

Donc,

$$\begin{aligned}
\sum_{n=k}^{\infty} p(n,k) X^n &= \sum_{n=k}^{\infty} (p(n, \leq k) - p(n, \leq k-1)) X^n, \\
&= \prod_{j=1}^{k} \frac{1}{1-X^j} - \prod_{j=1}^{k-1} \frac{1}{1-X^j}, \\
&= \prod_{j=1}^{k} \frac{1}{1-X^j} (1 - (1 - X^k)), \\
&= X^k \prod_{j=1}^{k} \frac{1}{1-X^j}.
\end{aligned}$$

■

CHAPITRE 3

LES APPLICATIONS DES FONCTIONS GÉNÉRATRICES

Manipuler les fonctions génératrices vous permettent de decider d'en quoi faire. A quelle niveau intervient elles ? La réponse en la trouve dans la littérature comme suit [18] :

Trouvez une formule exacte d'une suite de nombres : Pas toujours faisable, si votre suite est compliquée. Mais vous aurez au mois une bonne chance de trouver une telle formule.

Trouvez une formule de récurrence : Le plus souvent, les fonctions génératrices proviennent de formules de récurrence. Parfois, à partir de la fonction génératrice, vous trouverez une nouvelle formule de récurrence.

Trouvez des moyennes et d'autres propriétés statistiques : Les fonctions génératrices peuvent fournir des dérivations de divers aspects probabilistes du problème représenté par un suite inconnue.

Trouvez des formules asymptotiques : Vous trouverez ici certaines des applications les plus profondes et les plus puissantes de la théorie. Au lieu de chercher une formule exacte à des suites très difficile, on peut passer directement à la solution.

Prouver des identités : De très nombreuses identités sont connues en combinatoire et en mathématique. Les identités visées sont celles qui affirment qu'une certaine formule est égale à une autre formule.

Définition 3.0.10 *Un groupe $(G,*)$ est un ensemble G muni d'une loi de composition interne*

$$\begin{array}{ccc} G\times G & \longrightarrow & G \\ (a,b) & \longmapsto & a*b \end{array}$$

telle que :

1- *Il existe un élément neutre e : pour tout $a\in G, e*a=a*e=a$.*

2- *La loi est associative : pour tous $a,b,c\in G$, on a $(a*b)*c=a*(b*c)$.*

3- *Tout élément $a\in G$ a un inverse a' tel que $a*a'=a'*a=e$.*

La notation $(G,*)$ pour un groupe précise que la loi de groupe est notée $*$. Si la loi de groupe est la multiplication, le groupe est noté $(G,\times)$. L'élément neutre se note alors 1 et l'inverse de a se note a^{-1}. Pour un groupe $(G,+)$, l'élément neutre se note 0, et l'inverse d'un élément a se note $-a$. Si de plus la loi $*$ est commutative, alors $(G,*)$ est un groupe commutatif ou abélien.

Définition 3.0.11 *Un anneau (commutatif et unitaire) A est un groupe commutatif $(A,+)$ muni d'une deuxième loi de composition interne (appelée multiplication) vérifiant les conditions suivantes :*

1- *La multiplication est associative, commutative, et possède un élément neutre noté* 1.

2- *La multiplication est distributive par rapport à l'addition.*

Définition 3.0.12 *Un corps (commutatif) $\mathbb{K}$ est un anneau tel que tout élément non nul soit inversible pour la multiplication.*

Définition 3.0.13 *Un idéal I d'un anneau A est un sous-groupe de $(A, +)$ tel que I soit stable par la multiplication par les éléments de A, i. e*

$$x \in I \text{ et } \lambda \in A \Longrightarrow \lambda x \in I.$$

3.1 Application en combinatoire

Générer des fonctions peut être utile pour problèmes impliquant des fonctions de deux variable discrètes. On a choisit de travailler avec les coefficients binomiaux, afin d'arriver à construire la formule exacte qui calcul ces coefficients [18].
Soient n et k des entiers tels que $0 \leq k \leq n$. De combien de façon peut-on nous choisir de distribuer k boules sur n urnes ? Objectif : cherchant à introduire les fonctions génératrices.
Supposons que $f(n, k)$ soit le nombre de façons possibles. On procède par le principe des éléments distingués : divisant les en deux.

▹ Soit la $n^{\text{ème}}$ urne est vide, dans ce cas on distribue les k boule sur les $n-1$ urnes. Par conséquent, le nombre de façons possibles est $f(n-1, k-1)$.

▹ Soit la $n^{\text{ème}}$ urne contient une boule, dans ce cas on distribue les $k-1$ boule restantes sur les $n-1$ urnes. Par conséquent, le nombre de façons possibles est $f(n-1, k)$.

Les deux parties des urnes contenaient à l'origine $f(n, k)$. Il faut donc que $f(n, k)$ satisfont la récurrence de récurrence :

$$f(n, k) = f(n-1, k) + f(n-1, k-1), \qquad (f(n, 0) = 1). \tag{3.1}$$

Pour trouver la formule exacte recherché de ces nombres, nous utilisons la théorie des fonctions génératrices. Pour chaque n définissant la fonction génératrice ordinaire dont les coefficients représentent les $f(n,k)$.

$$B_n(X) = \sum_{k\geq 0} f(n,k)X^k. \tag{3.2}$$

Essayant, à partir de cette fonction de faciliter la recurrence en une formule simple :

$$\begin{aligned} B_n(X) &= \sum_{k\geq 0} f(n,k)X^k, \\ &= B_0(X) + \sum_{k\geq 1} f(n,k)X^k, \\ &= B_0(X) + \sum_{k\geq 1} f(n-1,k) + f(n-1,k-1)X^k, \end{aligned}$$

donc,

$$\begin{aligned} B_n(X) - B_0(X) &= \sum_{k\geq 1} f(n-1,k) + f(n-1,k-1)X^k, \\ &= \sum_{k\geq 1} f(n-1,k)X^k + \sum_{k\geq 1} f(n-1,k-1)X^k, \\ &= (\sum_{k\geq 0} f(n-1,k)X^k - B_0(X)) + X\sum_{k\geq 1} f(n-1,k-1)X^{k-1}, \\ &= (B_{n-1}(X) - B_0) + XB_{n-1}(X). \end{aligned}$$

Multipliez maintenant le deux cotés de l'égalité par X^k et faites la somme sur $k \geq 1$. Le résultat est

$$B_n(X) = (1+X)B_{n-1}(X)) \qquad (n \geq 1, B_0(X) = 1). \tag{3.3}$$

Ainsi,

$$B_n(X) = (1+X)^n. \tag{3.4}$$

Le nombre $f(n,k)$ se révèle être le coefficient de X^k dans le polynôme $(1+X)^n$. pour Trouver une formule pour $f(n,k)$, nous pourrions, par exemple, utiliser la formule de Taylor, qui nous dirait que $f(n,k)$ est la n$^{\text{ème}}$ dérivée de $(1+X)^n$ évaluée à $X = 0$, le tout divisé par $k!$. La différenciation est simple à réaliser, la k$^{\text{ème}}$ dérivée de $(1+X)^n$ est

$$(1 + X)^n = n(n-1)\cdots(n-k+1)(1+x)^{n-k}.$$

Si l'on met $X = 0$ et divisons par $k!$ nous découvrons rapidement que le nombre $f(n,k)$ est donnée par

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}. \tag{3.5}$$

pour les entiers n,k avec $0 \leq k \leq n$.

Ainsi,

$$\binom{-3}{3} = \frac{(-3)(-4)(-5)}{6} = -10, \qquad \binom{i}{2} = \frac{i(i-1)}{2}, \quad \text{etc.}$$

La fonctions génératrice est,

$$B_n(X) = (1+X)^n = \sum_{k\geq 0}\binom{n}{k}X^k = 1 + nX + \frac{n(n-1)}{2}X^2 + \cdots.$$

Bien évidement, on dit que $\binom{n}{k} \neq 0$ dans lequel $k \geq 0$.

Examinons le problème d'autre façon. Si nous multiplions $B_n(X)$ par y^n et sommons nous seulement sur $n \geq 0$, nous trouvons que

$$\sum_{n\geq 0} B_n(x)y^n = \sum_{n\geq 0}\sum_k \binom{n}{k}X^k y^n = \sum_{n\geq 0}(1+X)^n y^n = \frac{1}{1-y(1+x)}.$$

Ainsi

$$n \geq 0, \binom{n}{k} = \left[X^k y^n\right](1 - y(1 + X))^{-1}.$$

Avec $\left[X^k\right]$ représenter le coefficient binomial qui multiplie la variable X^k dans un polynôme. Plus précisément, $\left[X^k\right]P(X)$ représente le coefficient de X^k dans le polynôme $P(X)$.
Par exemple $\left[X^k\right]1/(1 - 3X) = 3^k$, $[X^m](1 + X)^s = \binom{s}{m}$.
Évaluons nous, pour un entier non négatif K, la somme $\sum_n \binom{n}{k}$.

$$\begin{aligned}\left[X^k\right]\sum_{n\geq 0}\sum_k \binom{n}{k} X^k y^n &= \left[X^k\right]\frac{1}{1 - y(1 + X)} = \frac{1}{1-y}\left[X^k\right]\frac{1}{1 - \left(\dfrac{y}{1-y}\right)X} \\ &= \frac{1}{1-y}\left(\frac{y}{1-y}\right)^k = \frac{y^k}{(1-y)^{k+1}}.\end{aligned}$$

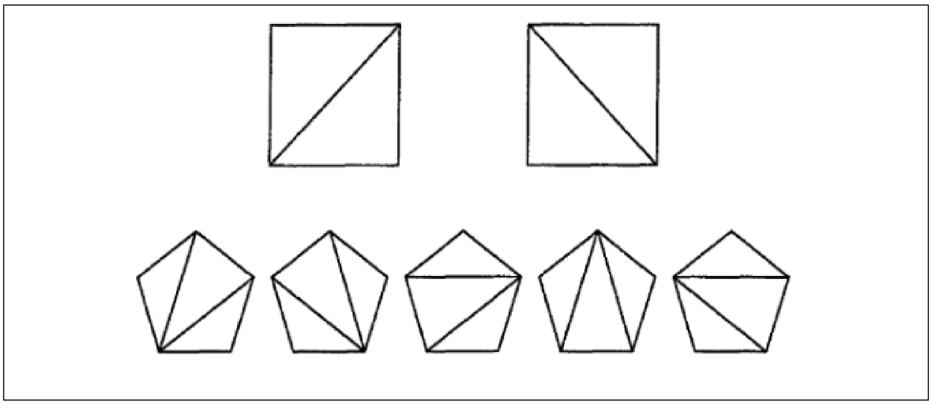
Consequence : Les deux formules implicites sont :

$$\sum_k \binom{n}{k} X^k = (1 + X)^n \quad ; \quad \sum_k \binom{n}{k} y^n = \frac{y^k}{(1-y)^{k+1}}.$$

3.2 Application en théorie des graphes

Il y a beaucoup de difficultés à compter des objets qui ont des symétries distinctes. Par exemple, si nous considérons comme égales les triangulations diagonales de polygones réguliers qui sont amenées l'une à l'autre par une rotation du polygone, l'obtention d'une formule exacte pour le nombre de triangulations deviendrait un problème compliqué, et la formule résultant n'apporterait rien de nouveau sur les triangulations, cela est du au fait que des triangulations distinctes possèdent des groupes de symétrie non isomorphes [11].

La numérotation des sommets d'un polygone simplifie sérieusement le problème n'a qu'un impact mineur sur la précision de la réponse, mais efficace dans de nombreux autres problèmes d'énumération. Nous commencerons par montrer comment elle est utilisée dans le l'énumération des nombre d'arbres possibles dans un graphe donné avec un nombre spécifié de sommets.



On utilise la notation $f(X)[X]$ pour le coefficient f_k dans la fonction génératrice.

Définition 3.2.1 *[11] Un graphe peut être défini comme un triple $\mathcal{T} = (V, E, I)$, où V représente l'ensemble fini des sommets du graphe, E représente l'ensemble des arêtes du graphe, qui relient les sommets entre eux, I est une fonction d'incidence qui associe chaque arête à une paire de sommets.*

Remarque 3.2.1 *La définition d'un graphe autorise différentes variables. Par exemple, il est parfois normal d'exiger qu'au plus une arête passe par chaque paire de sommets, et les boucles sont interdites (omises).*

Définition 3.2.2 1. *Deux sommets d'un graphe sont dits adjacents s'ils sont reliés par une arête.*

2. *Un graphe est dit connecté si pour toute paire $u, v \in V$ de ses sommets il existe une chaîne $(v_0 = u, v_1, v_2, ..., v_k = v \in V)$ des sommets de graphe telle que les deux sommets v_{i-1} et v_i sont adjcents pour chaque $i = 1, ..., k$.*

3. *Cycle : est une suite $v_1, v_2, ..., v_k \in V$ de sommets du graphe telle que les sommets v_i et v_{i-1} sont adjacents pour chaque $i = 1, ..., k$, tous les sommets $v_1, v_2, ..., v_{k-1}$ sont distincts et $v_0 = v_k$.*

4. *Arbre : est un graphe connecté sans cycles.*

5. *L'arbre enracinées est appelée ainsi car elle a un noeud spécial appelé "racine" qui représente le point de départ de l'arbre, à partir de la racine, chaque noeud peut avoir un ou plusieurs noeuds enfants.*

Tous les arbres à n sommets ($n \leq 5$) représentés sur la figure 3.1.

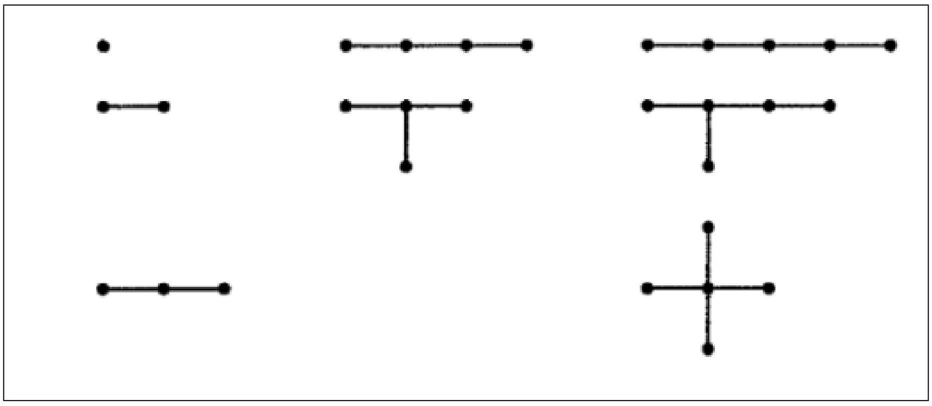


FIGURE 3.1: Tous les arbres avec $n \leq 5$ sommets.

.

L'énumération des arbres à n sommets est un problème compliqué car les arbres ont des symétries différentes. Nous allons aborder un problème plus simple, celui de l'énumération des arbres marquées.

Marquez chacun des sommets d'un arbre avec l'un des nombres de $\{1, 2, ..., n\}$ de manière à ce que des sommets distincts reçoivent des valeurs distingues.

Tous les arbres marquées avec $n \leq 4$ sommets sont illustrés à la figure 3.2.

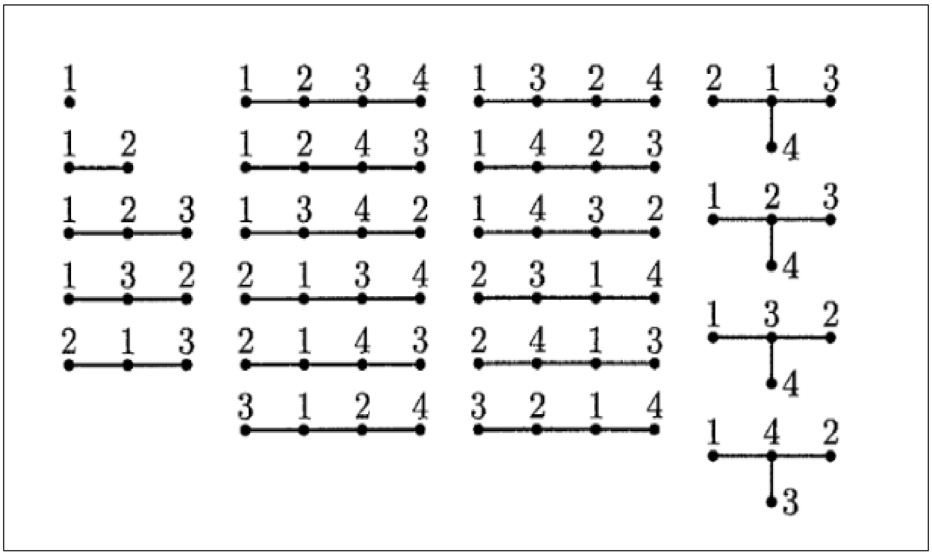


FIGURE 3.2: Tous les arbres marquées à n sommets ($n \leq 4$).

.

La suite des nombres d'arbres marquées avec n sommets commence par les nombres

$$1, 1, 3, 16, ...$$

On peut formuler le problème comme suit :
T_n : Le nombre d'arbres marquées ayant un sommet distingue, appelé la racine de l'arbre.
Il est clair que le nombre d'arbres marquées enracinées de n sommets est n fois le nombre d'arbres marquées à n sommets : il y a n choix différents de la racine.

Trouvons la fonction génératrice exponentielle pour le nombre d'arbres marquées enracinées :

$$T(X) = \sum_{n=1}^{\infty} \frac{1}{n!} T_n X^n = \frac{1}{1!}X + \frac{2}{2!}X^2 + \frac{9}{3!}X^3 + \frac{64}{4!}X^4 + \cdots \tag{3.6}$$

Après avoir supprimé la racine, l'arbre est divise en plusieurs nouveaux arbres et le nombre de ces nouveaux arbre coïncide avec racine, les nouveaux arbres peuvent également être considérés comme marqués : il suffit de remplacer les marques existantes $l_1, ..., l_i, l_1 < \cdots < l_i$ par les marques $1, ..., i$ en conservant leur ordre. Pour la racine d'une nouvelle arbre, on choisit le sommet adjacent à la racine de l'arbre initial. Par conséquent, à chaque arbre marquée enracinées avec une racine de valeur k nous avons associé un (multi) ensemble constitué de k arbres marquées enracinées. Nous parlons de multi-ensembles car certains des arbres nouvellement générés peuvent coïncider. Cette description implique que les arbres avec une racine de valeur $''k''$ sont énumérés par la fonction génératrice exponentielle $XT^k(X)$. En effet, les éléments

$$\frac{T_{l_1}}{l_1!} \cdots \frac{T_{l_k}}{l_k!} X^{l_1+\cdots+l_k}, \tag{3.7}$$

Tel que $l_1 + ... + l_k = n$ contribue au coefficient de X^{n+1} en $XT^k(X)$. L'ensemble des marques de $''n''$ sommets de $''k''$ arbres peut être divisé en "k" sous-ensemble disjoints contenant $l_1, ..., l_i$ marques de $\left(\binom{n}{l_1 ... l_k}\right) = \frac{n!}{l_1 ... l_k!}$ façon. Par conséquent, le nombre d'arbre enracinées marquées ayant $n + 1$ sommets et une racine de valeur $''k''$ est

$$n!\,[X^n]\,T^k(X) = \sum_{l_1+...+l_k=n} \frac{n!}{l_1!...l_k!} T_{l_1}...T_{l_k}. \tag{3.8}$$

Maintenant, en sommant les fonction T sur tout k, nous obtenons l'énoncé suivant.

Théorème 3.2.2 *La fonction génératrice exponentielle $T(X)$ pour le nombre d'arbre enracinées marquées en les énumérant par rapport au nombre d sommets satisfait l'équation de Lagrange*

$$T(X) = Xe^{T(s)}. \tag{3.9}$$

Maintenant, le théorème de Lagrange nous permet de calculer facilement le premier coefficient de la fonction $T(X)$. Par exemple, nous obtenons $T_5 = 625$,

$T_6 = 7776$.

Cependant, il serait bien d'avoir une formule explicite pour le coefficient. Pour obtenir une telle formule, nous aurons besoin d'une version plus précise du théorème de Lagrange.

Théorème 3.2.3 *Supposons que deux fonction $\varphi = \varphi(0)$, $\varphi(0) = 0$ et $\psi = \psi(t)$ sont liées par l'équation de Lagrange*

$$\varphi(X) = X\psi(\varphi(X)). \tag{3.10}$$

Alors le coefficient de X^n dans la fonction est

$$[X^n]\,\varphi(X) = \frac{1}{n}\left[t^{n+1}\right]\psi^n(t),$$

Appliquons ce résultat à l'eq (3.6) dont la solution est la fonction $T(X)$. On obtient

$$T_n = n!\,[X^n]\,T(X) = n!\left[t^{n-1}\right]e^{nt} = (n-1)!\frac{n^{n-1}}{(n-1)!} = n^{n-1}.$$

Par conséquent, nous avons démontré le résultat suivant.

Théorème 3.2.4 *Le nombre d'arbres marquées enracinées avec n sommets est $T_n = n^{n-1}$.*

Corollaire 3.2.1 *Le nombre d'arbres marquées à n sommets est n^{n-2}.*

Preuve. Pour une fonction $g(t)$ telle que $g(0) = 0$, $g'(0) = 0$, on a

$$\left[X^{-1}\right]f(X) = \left[t^{-1}\right]f(g(t))g'(t).$$

En effet, supposons $f(X) = f_{-m}X^{-m} + f_{-m+1}X^{-m+1} + ...,\ g(t) = g_1 t + g_2 t^2 + ...$ Pour $n \neq -1$ on a

$$\left[t^{-1}\right] g^n(t)g'(t) = \left[t^{-1}\right] \frac{1}{n+1}(g^{n+1}(t))' = 0,$$

puisque le reste de la dérivée d'une fonction est 0. Pour $n = -1$

$$\left[t^{-1}\right] f_{-1}\frac{1}{g(t)}g'(t) = f_{-1},$$

coefficient de X^n dans la fonction génératrice à la forme

$$[X^n]\,\varphi(X) = \left[X^{-1}\right] X^{n+1}\varphi(X),$$

réécrivez l'équation de Lagrange (3.10) lorsque la variable change

$$X = \frac{t}{\psi(t)}.$$

où $t = \varphi(X)$.

$$\begin{aligned}
\left[X^{-1}\right] X^{-n-1}\varphi(X) &= \left[t^{-1}\right] \frac{\psi^{n+1}(t)}{t^n}\frac{\psi(t) - t\psi'(t)}{\psi^2(t)}, \\
&= \left[t^{-1}\right]\left(\frac{\psi^n(t)}{t^n} - \frac{\psi^{n-1}(t)\psi'(t)}{t^{n-1}}\right), \\
&= \left[t^{n-1}\right]\psi^n(t) - \frac{1}{n}\left[t^{n-2}\right](\psi^n(t))', \\
&= \frac{1}{n}\left[t^{n-1}\right]\psi^n(t).
\end{aligned}$$

■

3.3 Application en statistique

Dans cette section, nous allons illustrer la puissance des fonctions génératrices dans l'étude d'une classe intéressante de processus stochastiques : les processus de branchement à l'époque victorienne, certaines personnes ont craint la disparition des noms des familles aristocratiques. Sir Francis Galton posa originellement la question de déterminer la probabilité d'un tel événement dans le Educational Times de 1873, et le Révérend Henry William Watson répondit avec une solution. Ensemble, ils écrivirent alors, en 1874, un article intitulé « On the probability of extinction of families » [16].

Leur modèle suppose (cela étant considéré comme allant de soi à l'époque de Galton, et étant encore le cas le plus courant dans la plupart des pays) que le nom de famille est transmis à tous les enfants mâles par leur père. Il suppose également que le nombre de fils d'un individu est une variable aléatoire à valeurs dans $\mathbb{N}$, et que le nombre de fils d'hommes différents sont des variables aléatoires indépendantes de même loi. Plus généralement, supposons qu'une population évolue par générations notons :

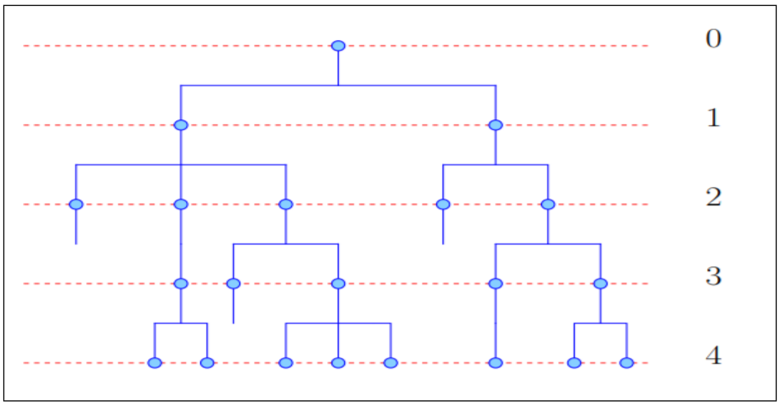
▹ Z_n : le nombre d'individus de la n$^{\text{ème}}$ génération. Chaque membre de la n$^{\text{ème}}$ génération donne naissance à une famille, éventuellement vide, de la génération suivante ; la taille de la famille est une variable aléatoire.

On fait les hypothèses suivantes [16] :

▹ Les tailles de chaque famille forment une collection de variable aléatoires indépendantes.

▹ Les tailles des familles suivent toutes la même loi.

Sous ces hypothèses, le processus est bien défini dès que la taille de la population initiale Z_0 est donnée, on supposera ici que $Z_0 = 1$. Ce modèle peut également représenter la croissance d'une population de cellules, celle de neutrons dans un réacteur, la propagation d'une maladie dans une population, etc.



On s'intéresse à la suite aléatoire $(Z_k)_{k=0}^n$ des tailles des générations successives. Ce processus peut être défini de la façon suivante : on considère une collection $\left(X_k^n\right)_{n\geq 0, k\geq 1}$ de variables aléatoires $(i.i.d)$.À valeurs dans $\mathbb{N}$.

▹ X_k^n : représente le nombre de fils du k$^{\text{ème}}$ individu de la n$^{\text{ème}}$ génération (si celui-ci existe).

▹ G : la fonction génératrice commune à ces variables aléatoires (encodant donc la loi du nombre de fils d'un individu). On peut alors poser $Z_0 = 1$ et pour $n \geq 1$,

$$Z_n = X_1^{n-1} + X_2^{n-1} + \cdots + X_{Z_{n-1}}^{n-1},$$

Définition 3.3.1 *Soit X une variable aléatoire à valeur dans $\mathbb{N}$ on appelle fonction génératrice de X la fonction*

$G_X : \mathbb{N} \to \mathbb{N}$ *donnée par la série entière*

$$G_X(s) = E(s^X) = \sum_{k=0}^{n} f_X(k)s^k.$$

Avec la fonction de masse de X donne lieu à la suite $(f_X(k))_{k=0}^{\infty}$ tels que $f_X : \mathbb{R} \to [0, 1]$ donnée par $f_X(k) = \mathbb{P}(X = k)$.

Le nombre d'individus de la n$^{\text{ème}}$ génération étant égal au nombre total de fils individus de la (n-1)$^{\text{ème}}$ génération. On notera $G_Z(s) = E(s^{Z_n})$ la fonction génératrice de Z_n. Observez qu'en particulier $G_1 = G$, puisque $Z_0 = 1$.
L'étude du processus au temps n ne requiert qu'un espace de probabilité discret (les trajectoires du processus entre les temps 0 et n).

On utilise le téorème d'Abel : le théorème d'Able fournit une technique efficace pour calculer les moment de X.

$$G'_X(s) = \sum_{k=0}^{\infty} k s^{k-1} f_X(k) \quad \Rightarrow \quad G'_X(1) = E(X),$$

$$G''_X(s) = \sum_{k=0}^{\infty} k(k-1) s^{k-2} f_X(k) \quad \Rightarrow \quad G''_X(1) = E(X(X-1)),$$

$$G^{(l)}_X(s) = \sum_{k=0}^{\infty} k \cdots (k-l+1) s^{k-l} f_X(k) \quad \Rightarrow \quad G^{(l)}_X(1) = E(X \cdots (X-l+1)).$$

Proposition 3.3.1 *Si $G_X(s)$ est la fonction génératrice de X, alors*

$$E(X) = G'_X(1), \qquad Var(X) = G''_X(1) + G'_X(1) - G'_X(1)^2.$$

Les expressions dans les membres de droit devant être compris comme des limites $s \uparrow 1$ lorsque le rayon de convergence de G_X est égal à 1.

Lemme 3.3.1 *Soit $X = (X_1, ..., X_n)$ un vecteur aléatoire discret et $\varphi : \mathbb{R}^n \to \mathbb{R}$, avec $\varphi(X)$ définit une variable aléatoire discrète. Alors,*

$$E(\varphi(X)) = \sum_{x \in X(\Omega)} \varphi(X) f_X(X),$$

dés que cette somme est absolument convergent.

Preuve. Notons $E = X(\Omega)$, $F = \varphi(E)$ et $Y = \varphi(X)$. On a

$$\begin{aligned} E(Y) &= \sum_{y\in F} yP(Y=y) = \sum_{y\in F} yP(\varphi(X)=y), \\ &= \sum_{y\in F} yP(X\in\varphi^{-1}(y)) = \sum_{y\in F} y \sum_{X\in\varphi^{-1}(y)} P(X=x), \\ &= \sum_{y\in F, x\in E, \varphi(x)=y} yP(X=x) = \sum_{x\in E} \varphi(X)P(X=x). \end{aligned}$$

Observez que la convergence absolue de la série est cruciale pour pouvoir réorganiser les termes comme on l'a fait. ■

Définition 3.3.2 *Soient X, Y deux variable aléatoir discrètes. On appelle espérance conditionnelle de Y étant données X la variable aléatoire*

$$E(Y \mid X)(.) \equiv E(Y \mid X = .) = \sum_{y\in Y(\Omega)} y f_{Y|X}(Y \mid .),$$

pourvu que $\sum_{y\in Y(\Omega)} |y| f_{Y|X}(Y \mid .) < \infty$.

Lemme 3.3.2 *L'espérance conditionnelle $E(Y \mid X)$ satisfait*

$$E(E(Y \mid X)) = E(Y),$$

plus généralement, pour toute fonction $\varphi : \mathbb{R} \to \mathbb{R}$ telle que les espérance existent,

$$E(E(Y \mid X)\varphi(X) = E(Y\varphi(X)).$$

Preuve. La première affirmation est un cas particulier de la seconde : il suffit de choisir $\varphi \equiv 1$. Démontrons donc la seconde affirmation. Il suit du lemme

(3.3.1) que

$$\begin{aligned} E(E(Y \mid X)\varphi(X)) &= \sum_{x,y} y f_{Y|X}(y \mid x)\varphi(x) f_X(x), \\ &= \sum_{x,y} y\varphi(x) f_{x,y}(x,y) = E(Y\varphi(X)). \end{aligned}$$

■

Proposition 3.3.2 *Soient* $(X_1, X_2, ...)$ *une suite de variables aléatoires* (*i.i.d*) *à valeurs dans* $\mathbb{N}$, G_X *leur fonction génératrice commune, et* $\mathbb{N}$ *une variable aléatoire à valeurs dans* $\mathbb{N}^*$, *indépendants des* X_i *et dans la fonction génératrice est* G_N. *Alors la fonction génératrice de* $S = X_1 + \cdots + X_N$ *est donnée par*

$$G_s = G_N \circ G_X.$$

Preuve. En utilisant le lemme (3.4.2),

$$\begin{aligned} G_S(s) &= E(s^s) = E((E(s^s \mid N))) = \sum_n E(s^s \mid N)(n) = P(N = n), \\ &= \sum_n E(s^{X_1+...+X_n})P(N = n) = \sum_n E(s^{X_1})...E(s^{X_n})P(N = n), \\ &= \sum_n (G_X(s))^n P(N = n) = G_N(G_X(s)). \end{aligned}$$

■

Théorème 3.3.1 *Pour tout* $n \geq 1$,

$$G_n = G^{\circ n} \equiv G \circ G \circ \cdots \circ G.$$

Preuve. Soit $n \geq 1$. Il suit immédiatement de la Proposition (3.3.2) que

$$G_n = G_{n-1} \circ G,$$

puisque Z_n est la somme de Z_{n-1} variables aléatoires (*i.i.d*) de fonction génératrice G. L'affirmation se démontre alors en itérant précédent :

$$G_n = G_{n-1} \circ G = (G_{n-2} \circ G) \circ G = \cdots = G \circ G \circ \cdots \circ G.$$

■ Les moments de la variable aléatoire Z_n peuvent facilement s'exprime en termes des moments de la variable aléatoire Z_1 décrivant la taille d'une famille typique.

Lemme 3.3.3 *Soit* $\mu = E(Z_1)$ *et* $\sigma^2 = Var(Z_1)$. *Alors*

$$\begin{aligned} E(Z_n) &= \mu^n, \\ Var(Z_n) &= \begin{cases} n\sigma^2 & si \mu = 1 \\ \sigma^2(\mu^n - 1)\mu^{n-1}(\mu - 1)^{-1} & si \mu \neq 1. \end{cases} \end{aligned}$$

Preuve. Par le Théorème (3.3.1), $G_n = G^{\circ n} = G \circ G^{\circ(n-1)} = G \circ G_{n-1}$. Par conséquent,suit de la proposition (1. 3. 2) que

$$E(Z_n) = G_n'(1) = G'(G_{n-1})G_{n-1}'(1) = G'(1)G_{n-1}(1) = \mu E(Z_{n-1}),$$

ce qui donne bien, après itération, $E(Z_n) = \mu^n$. Similairement,

$$G_n''(1) = G''(1) = (G_{n-1}'(1))^2 + G'(1)G_{n-1}''.$$

Par conséquent, la Proposition(3.3.1) implique que

$$Var(Z_n) = \sigma^2\mu^{2n-2} + \mu Var(Z_{n-1}).$$

■

Et la conclusion suit. Une question particulièrement intéressante concerne le destin de la population : va-t-elle s'éteindre après un temps fini, ou au contraire, toutes les générations auront-elles une taille strictement positive ? Cette question peut être reformulée sous la forme suivante : la limite $\lim_{n\to\infty} P(Z_n = 0)$ est-elle égale à 1 (extinction inéluctable) ou strictement inférieure à 1 (survie possible) ? (Observez que s'il est possible qu'un individu n'ait pas de descendance, alors la probabilité d'extinction est toujours strictement positive).

Remarque 3.3.2 *Dans ce cas, " l'événement la population s'éteint après un temps fini pourrait s'écrire " (puisque $Z_n \in \mathbb{N}$ pour tout n)*

$$\{extinction\} = \left\{ \lim_{n\to+\infty} Z_n = \right\} = \{\exists n_0 : Z_n = 0, \forall n \geq n_0\} = \bigcup_{n\geq 1} \{Z_n = 0\} .$$

De plus, cette mesure limite satisfera $\mathbb{P}(\lim_{n\to\infty} Z_n = 0) = \lim_{n\to\infty} \mathbb{P}(Z_n = 0)$, car la suite d'événements $\{Z_n = 0\}_1$ est croissante.

Le théorème suivant montre que le destin de la population est étroitement lié à la taille moyennes des familles.

Théorème 3.3.3 *Soit $\mu = E(Z_1)$, la taille moyenne d'une famille. La probabilité d'extinction*

$$\eta = \lim_{n\to\infty} \mathbb{P}(Z_n = 0), \tag{3.11}$$

est donnée par la plus petite racine positive de l'equation $s = G(s)$. En particulier, $\eta = 1$ si $\mu < 1$ et $\eta < 1$ si $\mu > 1$. Lorsque $\mu = 1$, on a $\eta = 1$ dès que loi de Z_1 possède une variance positive.

Preuve. Notons $\eta_n = \mathbb{P}(Z_n = 0) = G_n(0)$. L'existence de la limite $\eta = \lim_{n\to\infty} \eta_n$ est immédiate puisque $(\eta_n)_{n\geq 1}$ est une suite croissante et bornée (par 1).On a

$$\eta_n = G_n(0) = G(G_{n-1}(0)) = G(\eta_{n-1}).$$

Par continuité de G, on peut passer à la limite ($n \to \infty$), ce qui montre que la probabilité d'extinction satisfait

$$\eta = \lim_{n\to\infty} \eta_n = \lim_{n\to\infty} G(\eta_{n-1})G(\lim_{n\to\infty} \eta_{n-1}) = G(\eta).$$

Vérifions à présent que si a est racine positive de cette équation, alors $\eta \leq a$. G étant croissante sur $[0, 1]$, on a

$$\eta_1 = G(0) \leq G(a) = a.$$

Similairement

$$\eta_2 = G(\eta_1) \leq G(a) = a.$$

Il suit, par induction, que $\eta_n \leq a$, pour tout n, et donc que $\eta \leq a$. Par conséquent, η est bien la plus petite racine positive de l'équation $s = G(s)$.
Pour démontrer la seconde affirmation, on utilise le fait que G est convexe sur $[0, 1]$, ceci est vrai, car

$$G''(s) = E(Z_1(Z_1-1)s^{Z_1-2}) = \sum_{k\geq 2} k(k-1)s^{k-2}\mathbb{P}(Z_1 = k) \geq 0, \quad \text{pour } s \in [0, 1].$$

G est donc convexe (en fait, strictement convexe si $\mathbb{P}(Z_1 \geq 2) > 0$) et croissante sur $[0, 1]$, avec $G(1) = 1$. L'équation $s = G(s)$ possède toujours au moins une solution en $s = 1$ et au plus une seconde (par convexité), sauf dans le cas trivial où $\mathbb{P}(Z_1 = 1) = 1$, pour lequel $G(s) = s$ pour tout s et $\eta = 0$. En excluant ce dernier cas, la question est donc de déterminer si une seconde solution inférieure à 1 existe (lorsqu'elle existe, elle est forcément positive, car $G(0) \geq 0$). Un coup d'oeil à la figure (3.3), montre que cela déponde de la valeur de $\mu = G'(1)$. Lorsque $\mu = G'(1) < 1$ la plus petite solution est $\eta = 1$ lorsque $\mu = G'(1) > 1$, la plus petite solution doit être inférieure à 1, puisque $G(0) \geq 0$, et donc $\eta < 1$. Finalment, dans le cas $\mu = 1$, le deux courbes sont tangentes en 1, et donc $\eta = 1$ dès que Z_1 possède une variance positive (puisque dans ce cas G est strictement convenxe $[0, 1]$). ■

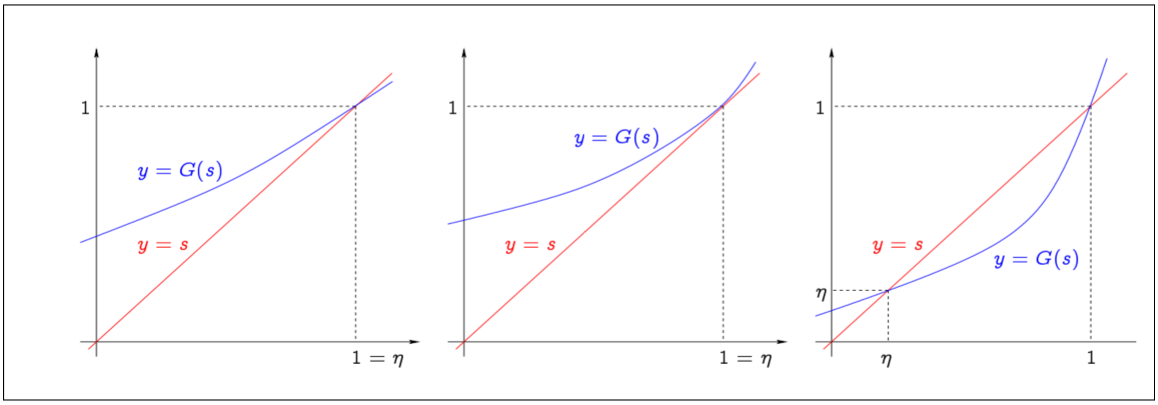


FIGURE 3.3: La solutions de l'équation $G(s) = s$. Gauche : $\mu < 1$. Milieu : $\mu = 1$ et $VAr(Z_1) > 0$. Droite : $\mu > 1$.

3.4 Application en informatique.

La théorie des codes correcteurs d'erreurs fournit une application de la théorie des corps finis aux télécommunications. Le problème est de savoir comment, lorsque des données sont transmises sur des réseaux, des erreurs de transmission peuvent survenir et affecter l'intégrité et la validité des données transmises, entraînant une perte partielle ou totale de ces données en raison d'interférences de signal ou d'une mauvaise qualité de communication. Pour résoudre ces problèmes, nous utilisons le correcteur **Bose-Chaudhuri-Hocquenghem**.

Le **BCH** est un type de code correcteur d'erreurs utilisé dans les système de communication pour détecter et corriger les erreurs de transmission. Il offre une fiabilité accrue en assurant l'intégrité des données transmises [15]. Dans toute la suite soit $\mathbb{K}$ un corps fini à q éléments de caractéristique p.

Définition 3.4.1 *Soient $x = (x_1, ..., x_n)$, $y = (y_1, ..., y_n)$ des éléments de $\mathbb{K}^n$. La fonction de Hamming $h(x, y)$ entre x et y est le nombre d'indices i, avec $1 \leqslant i \leqslant n$, tels que $X_i \neq y_i$. Le poids de Hamming $w(x)$ est par définition $h(x, 0)$.*

Proposition 3.4.1 *La fonction de Hamming est une distance sur $\mathbb{K}^n$.*

Supposons que l'on ait à transmettre des données, et que ces données soient exprimées comme une suite de h éléments de $\mathbb{K}$. On appellera cette suite l'information initiale. Lors du processus de transmission des erreurs peuvent se produire. La question qui se pose est de reconstituer l'information initiale à partir des données reçues. À cette fin on commence par adjoindre des données supplémentaires à l'information initiale, on peut y ajouter $n - h$ éléments de $\mathbb{K}$, déterminés par la suite initiale. On peut par exemple répéter le message deux ou trois fois ! De façon plus générale on peut déterminer une suite, plus longue, de n éléments de $\mathbb{K}$ à partir de la suite initiale. Celle-ci n'apparaît pas nécessairement explicitement dans la suite finale qui doit satisfaire à certaines relations. On appellera cette suite les données transmises. Comme elles sont déterminées par l'information initiale, elles doivent satisfaire à certaines relations. Dans l'exemple donné, il doit y avoir répétition des suites de symboles. S'il y a erreur durant la transmission les données reçues différent des données transmises. Ceci se détecte en observant si les données reçues satisfont ou non aux relations mentionnées plus haut. C'est ici qu'intervient la distance de Hamming. On considère la différence entre les données transmises et celles qui ont été reçues. Supposons que le nombre d'erreurs soit petit, disons inférieur à un entier fixé t. Les données transmises se trouvent à distance (pour la distance de Hamming) moins que t des données reçues. Si dans une boule de rayon t autour des données reçues il y a un seul élément qui satisfait aux relations imposées on a reconstitué les données transmises. Dans le processus décrit on a donc à la source un espace $\mathbb{K}^h$ correspondant à l'information initiale, à l'arrivée un espace $\mathbb{K}^n$ correspondant aux données transmises et reçues, une application f de $\mathbb{K}^h$ dans $\mathbb{K}^n$ correspondant au processus de transmission théorique (sans altération).

Définition 3.4.2 *Le sous-ensemble $\mathbb{K}^n$ image de f est appelé le code.*

Enfin on a une autre application g de $\mathbb{K}^h$ dans $\mathbb{K}^n$ correspondant au processus de transmission réel, dans lequel il y a altération. La question de savoir quand on peut déterminer f à partir de g.

Définition 3.4.3 *L'ensemble C est par définition le code, un élément de C est un mot. L'entier h est la dimension du code, l'entier n est la longueur du code.*

Un code est dit linéaire si l'ensemble C est un sous-espace vectoriel de $\mathbb{K}^n$, on le supposera de dimension h. Une matrice (h, n) à coefficients dans $\mathbb{K}$ dont les vecteurs lignes engendrent le code sera appelée une matrice génératrice du code, on la notera G. Une matrice $(n - h, n)$ à coefficients dans $\mathbb{K}^h$ dont les vecteurs lignes constituent un système d'équations pour le code sera appelée une matrice de parité du code, on la notera H. Supposons que le processus de transmission réel g fasse au plus t erreurs. Soit x un élément de. S'il n'y a qu'un point du code dans la boule de centre $g(x)$ et de rayon t, ce point est $f(x)$. Ce sont nécessairement les dormées transmises. On dit alors que le code C peut corriger jusqu'à t erreurs. Précisons comment ceci peut être assuré.

Définition 3.4.4 *On appelle distance minimale du code C la quantité :*

$$\delta_c = min_{x,y \in c, x \neq y} h(x, y).$$

Dans le cas d'un code linéaire le code est un sous-espace vectoriel de dimension h de $\mathbb{K}^n$, dans ce cas la distance minimale est le poids minimal d'un élément non nul. Pour le montrer il suffit de faire une translation : pour $x, y \in C$ on a $h(x, y) = w(x - y)$.

Proposition 3.4.2 *Si la distance minimum δ_c d'un code C est inférieure ou égale à* $2t + 1$, *le code peut corriger jusqu'à t erreurs*

Preuve. La condition dit que dans une boule fermée de rayon t il y a au plus un élément du code. Donc si on a transmis des données, et qu'au plus t erreurs ont été commises, l'inégalité triangulaire montre que dans la boule qui a pour centre les données reçues et de rayon t, il y a un élément du code et un seul. Ce sont les données transmises. ■

Proposition 3.4.3 *Un code linéaire de matrice de parité H est de distance minimale δ supérieure ou égale à $d+1$ si et seulement si tout système de d colonnes de la matrice de parité H est linéairement indépendant.*

Preuve. Puisque le code est linéaire il suffit d'évaluer le poids minimal d'un vecteur non nul du code. Dire que la distance minimale δ est supérieure ou égale à $d+1$ équivaut donc à dire qu'il n'existe pas de vecteur non nul dans le code qui appartienne à la boule de centre 0 et de rayon d. Soit qu'il n'existe pas de vecteurs non nul dans le code ayant au plus d coordonnées non nulles. Les vecteurs lignes de la matrice de parité sont les coefficients des formes linéaires définissant le code. Dire qu'il y a un élément non nul du code qui a au plus d coordonnées non nulles équivaut donc à dire que l'on peut trouver une relation linéaire non triviale entre d colonnes de la matrice de parité. Les coefficients de cette relation linéaire sont les coordonnées du vecteur considéré. Donc dire que la distance minimale est supérieure ou égale à $d+1$ équivaut à dire que tout système de d colonnes de la matrice de parité est libre. ■

On va dans la suite décrire deux types de code, et ce dans un des cas jusqu'au décodage. Cela permettra d'illustrer des techniques diverses d'algèbre, aucune n'est compliquée en elle-même, c'est leur succession qui rend le problème délicat.

Définition 3.4.5 *On dira qu'un code C de longueur n est cyclique si et seulement*

$$(a_1 \ldots, a_n) \in C \Rightarrow (a_n \ldots a_1, a_{n-1}) \in C.$$

On va donner une interprétation multiplicative des codes cycliques. Considérons l'anneau quotient $K[X]/(X^n-1)$, l'application linéaire

$$\begin{array}{rcl} \psi : \mathbb{K}^n & \longrightarrow & K[X]/(X^n-1), \\ (a_1, ..., a_n) & \mapsto & a_1 + a_2X + ... + a_nX^{n-1}, \end{array}$$

est bijective.

Proposition 3.4.4 *Soit C un code dans $\mathbb{K}^n$, C est cyclique si et seulement si $\psi(C)$ est un idéal.*

Preuve. En effet, si la classe d'un polynôme P est dans le code, vu comme idéal de $\mathbb{K}[X]/(X^n-1)$. Il en est de même pour la classe XP. Ce qui veut exactement dire que si $(a_1, ..., a_n) \in C$, il en est de même pour $(a_n, a_1..., a_{n-1})$. Inversement, cette dernière condition, interprétant cette suite comme la classe d'un polynôme P, signifie que si P est dans le code, il en est de même pour XP et plus généralement pour RP, où R est un polynôme quelconque. ■

Nous étudions maintenant le code **BCH**. Une façon commode de déterminer un idéal dans $\mathbb{K}[X]$ est de le construire comme ensemble des polynômes qui ont pour racines certains éléments d'une extension algébrique $\mathbb{L}$ de $\mathbb{K}$. Puis on peut considérer l'image dans l'anneau quotient $\mathbb{K}[X]/(X^n-1)$, comme l'application est surjective c'est un idéal. Si les éléments considérés dans $\mathbb{L}$ sont des racines n-ième de 1, la valeur prise par un élément d'une classe modulo X^n-1 ne dépend que de la classe et non de l'élément. On peut donc directement définir un idéal dans $\mathbb{K}[X]/(X^n-1)$ comme étant l'ensemble de classes prenant la valeur 0 sur certaines racines n-ièmes de 1. Choisissons donc une racine primitive n-iémes de 1, soit μ dans un corps $\mathbb{L}$ de caractéristique p, on suppose évidemment que n est premier à la caractéristique p. Pour que $\mathbb{L}$ contienne des racines primitives n-iémes de l'unité if faut et il suffit que n divise $q-1$. Considérons l'idéal des classes de polynômes s'annulant sur $\mu^b,...,\mu^{b+d-2}$.

On suppose que ces racines sont deux à deux distinctes, c'est-à-dire qu l'on suppose que l'ordre n de μ dans le groupe multiplicatif $\mathbb{L}^*$ est supérieur ou égal à d [15].

On peut évidemment aussi considérer les polynômes nuls sur ces racines, ce sont ceux divisibles par le ppcm des polynômes minimaux des $\mu^i, b \leqslant i \leqslant b+d-2$, qui est le polynôme générateur du code. Un code déterminé par un idéal de ce type est appelé un code **BCH**. À cause de la proposition suivante on dit qu'il est de distance prescrite d. Avec

▹ b : fait référence au début de la plage d'indices.

▹ d : représente la distance minimale du code.

▹ i : est un indice de position.

Proposition 3.4.5 *Un code* ***BCH*** *est de distance minimale au moins d. Si* $d = 2t+1$ *il peut donc corriger jusqu'à t erreurs.*

Preuve. En effet, on doit vérifier qu'il n'y a pas, dans le code, de vecteurs non nuls ayant moins de d coordonnées non nulles. Identifions un vecteur à un polynôme non nul $P = a_1 + a_2X + ... + a_{n-1}X^{n-1}$. On doit vérifier que les équations $P(\mu^i) = 0$, avec $b \leqslant i \leqslant b+d-2$ ont lieu si le polynôme a au moins d coefficient non nuls. On a $d-1$ équations à n inconnues et la matrice du système linéaire est la suivant :

$$\begin{pmatrix} 1 & \mu^b & \cdots & \mu^{b(n-1)} \\ 1 & \mu^{b+1} & \cdots & \mu^{b(n+1)(n-1)} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \mu^{b+d-2} & \cdots & \mu^{(b+d-2)(n-1)} \end{pmatrix}$$

Si on sélectionne $d-1$ colonnes quelconques, on reconnît, à un facteur multiplicatif près, un déterminant de van der Monde qui est non nul. Si bien que $d-1$ colonnes quelconques de cette matrice sont linéairement indépendantes.

Donc un élément non nul dans le code doit avoir au moins d coordonnées non nulles. Donc si P n'a que $d-1$ coefficients éventuellement non nuls, il est nul. ■

Remarque 3.4.1 *Dans le cas des codes* **BCH**, *la matrice de Van der Monde est utilisée pour construire la matrice de contrôle de parité, également appelée matrice de syndromes. La matrice de contôle de parité est une matrice utilisée pour détecter et localiser les erreurs dans les données transmises.*
En utilisant la matrice de contrôle de parité, il est possible de calculer les syndromes pour un mot de code donnée.
▹ *Les syndromes sont des valeurs calculées à partir des données reçues et de la matrice de contrôle de parité. En comparant les syndromes avec un tableau de syndromes précalculés pour différents schémas d'erreur, il est possible de déterminer les positions et les valeurs des erreurs.*

Supposons que l'on ait le code **BCH** de longueur n et de distance minimale au moins égale à $d = 2t + 1$ défini plus haut. Supposons que le processus de transmission des données fasse au plus t erreurs, si bien que le code peut corriger ces erreurs, soit $\mathbb{R} \in K[X] \diagup (X^n - 1)$ les données reçues, cherchons à déterminer les données transmise. Considérons la différence, que l'on appellera le polynôme d'erreur, $E = R - T$ entre les données transmise T et les données reçues R. On va procéder en deux étapes, d'abord on va déterminer en quels emplacements se sont produites les erreurs, puis on les déterminera.
Les valeurs $R(\mu^i)$ pour $b \leqslant i \leqslant b + d - 2$ sont connues, par construction on a $E(\mu^i) = R(\mu^i)$ pour $b \leqslant i \leqslant b + d - 2$. Les coefficients de E sont donc solutions d'un système linéaire de $d - 1$ équations et n inconnues (les coefficients du polynôme E). Il y a au moins une solution par hypothèse, mais en général il y a plusieures. Pour déterminer la bonne on procède comme suit. Établissons d'abord un lemme.

Considérons un entier $u \leqslant t$ un entier, et un polynôme :

$$F = \sum_{i=0,\dots,u-1} f_i X^{a'_i},$$

où les exposants sont a'_j deux à deux distincts et strictement inférieurs à n. Les coefficients $f_i \in K$ ne sont pas nécessairement non nuls. Posons $y_j = \mu^{a'_j}$ et posons :

$$\prod_{j=1,\dots,u} (X - y_j) = \sum_{l=0,\dots,u} \alpha_{u-l} X^l.$$

Si, dans ce polynôme, on substitue la valeur y_j à la variable X, on obtient :

$$\sum_{l=0,\dots,u} \alpha_{u-l} y_j^l = 0.$$

Multiplions cette équation par $f_j y_j^k$, pour $b \leqslant k \leqslant b + d - 2$, sommons sur j, nous obtenons, par définition de F, la relation suivante :

$$\alpha_u F(\mu^k) + \alpha_{u-1} F(\mu^{k+1}) + \cdots + \alpha_1 F(\mu^{k+u-1}) + F(\mu^{k+u}) = 0,$$

avec

▹ $F(\mu)$: est une fonction représentant les symboles émis.

▹ α_u : est un coefficient spécifique utilisé dans les calculs d'erreurs **BCH**.

▹ μ : est un entier qui détermine le champ logique sur lequel le codeur d'erreurs fonctionne.

▹ k : est la position de l'erreur dans le symbole émis.

▹ u : est le nombre d'erreurs à corriger.

On obtient donc un système de $d - 1$ équation linéaires en les u inconnues α_j.

Lemme 3.4.1 *Le système linéaire précédent admet une solution unique seulement si les coefficients de f_j de F sont tous non nuls.*

Preuve. Nous ne discutons pas ici l'existence mais seulement l'unicité de la solution. Pour étudier cette question, sélectionnons les u premières équations parmi les $d-1$ équations données. On obtient comme matrice du système :

$$\begin{pmatrix} F(\mu^b) & F(\mu^{b+1}) & ... & F(\mu^{b+u-1}) \\ F(\mu^{b+1}) & F(\mu^{b+2}) & ... & F(\mu^{b+u}) \\ \vdots & \vdots & & \vdots \\ F(\mu^{b+u-1}) & F(\mu^{b+1}) & ... & F(\mu^{b+2u-1}) \end{pmatrix}$$

Or cette matrice est égale au produit suivant VDV^t où on a

$$V = \begin{pmatrix} 1 & 1 & ... & 1 \\ y_1 & y_2 & ... & y_u \\ \vdots & \vdots & & \vdots \\ y_1^{u-1} & y_2^{u-1} & ... & y_u^{u-1} \end{pmatrix} \quad et \quad D = \begin{pmatrix} f_1 y_1^{u-1} & 0 & ... & 0 \\ 0 & f_2 y_2^{u-1} & \ddots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & ... & 0 & f_u y_u^{u-1} \end{pmatrix}$$

Donc le déterminant de la matrice du système est égal à

$$f_1 \cdots f_u (y_1 \cdots y_u)^{u-1} \prod_{0 \leqslant i < j \leqslant u} (y_i - y_j)^2.$$

Comme les racines y_i sont supposées deux à deux distinctes se déterminant est non nul si et seulement si tous les coefficients f_i sont non nuls. ∎

Appliquons ces résultats au polynôme d'erreur E, supposons que r erreurs aient été commises, avec $r \leqslant t$, et soit enfin $u \leqslant t$. Considérons le déterminant :

$$D_u = \begin{vmatrix} E(\mu^b) & E(\mu^{b+1}) & ... & E(\mu^{b+u-1}) \\ E(\mu^{b+1}) & E(\mu^{b+2}) & ... & E(\mu^{b+u}) \\ \vdots & \vdots & & \vdots \\ E(\mu^{b+u-1}) & E(\mu^{b+1}) & ... & E(\mu^{b+2u-1}) \end{vmatrix}$$

On a :

Corollaire 3.4.1 *Le déterminant D_u, $1 \leqslant u \leqslant t$, est nul dès que $u > r$, il est non nul pour $u = r$.*

Pour déterminer le nombre d'erreur commises on doit donc calculer ces déterminants et calculer le plus grands valeur inférieure ou égale à t pour laquelle il est non nul.
On calcule alors le polynôme d'erreurs comme suit. posons

$$E = \sum_{i=0,\dots,r} e_i X^{a_i},$$

avec
▹ E : représente les symboles de récupération utilisés dans le code **BCH**. Ces symboles supplémentaires sont utilisés pour récupérer les données manquantes.
▹ e_i : est un ensemble d'éléments dans un corps de Galois (un corps de Galois est un corps fini dans lequel les opérations de l'addition, de la soustraction, de la multiplication et de la division sont définies, il est caractérisé par un nombre fini). Il définit la valeur du symbole individuel à la position i.
▹ X : est la variable algébrique utilisée dans le code **BCH**.
▹ a_i : représente des nombres binaires utilisés pour déterminer la position du symbole dans la matrice.
Avec $r \leqslant t$, $e_i \in \mathbb{K}^*$ et les entiers a_i deux à deux distincts et strictement inférieurs à n. Les entiers a_i correspondent aux emplacements où se sont produites les erreurs. Posons $x_i = \mu^{a_i}$ et considérons le polynôme à coefficients dans $\mathbb{L}$:

$$\prod_{i=1,\dots,e} (X - x_i) = \sum_{j=0,\dots,e} \tau_{e-j} X^j.$$

Si, dans ce polynôme on substitue à la variable X la valeur x_i, puis si on somme su i on obtint comme précédemment un système linéaire :

$$\tau_r E(\mu^k) + \tau_{\tau-1} E(\mu^{k+1}) + ... + \tau_1 E(\mu^{k+r-1}) + E(\mu^{k+r}) = 0,$$

avec

▹ $E(\mu^k)$: représente les symboles de récupération dans le code **BCH**.

▹ $\tau_r, \tau_{r-1}, \tau_1$: représentent les facteurs de correction utilisées dans le code **BCH**.

▹ $\mu^k, \mu^{k+1}, ..., \mu^{k+r}$: définissent les positions des symboles dans la matrice.

pour $k = b, ..., b + r - 1$. On peut donc calculer la valeur des τ_i qui sont, au signe près, les fonctions symétrique élémentaires des x_i. Précisément $(-1)^i \tau_i$ est la i-ième fonction symétrique élémentaire des racines x_i, si bien que l'on obtient ces racines en résolvant l'équation :

$$X^r + \tau_1 X^{r-1} + ... + \tau_r = 0.$$

Notons que l'on peut toujours résoudre une telle équation, quitte à tester tous les éléments du corps fini $\mathbb{L}$!

Enfin, on calculer les coefficient e_i en résolvant le système linéaire :

$$\sum_{1 \leqslant i \leqslant r} e_i \mu^{j(a_i)} = R(\mu^j).$$

CONCLUSION

Ce travail est une étude qui consiste à travailler sur un outil de calcul puissant en mathématiques. Cet outil s'appel les fonctions génératrices. Le rôle principal de ces fonctions est de fournir une méthode ou une formule suffisante et efficace pour résoudre des problèmes de structures discrètes dans le domain de la combinatoire. Dans certains cas et malheureusement, ces fonctions peuvent être devant des difficultés de calcul en vertus de leurs complexités et leurs dépendances aux paramètres. Il est important de comprendre les avantages et les inconvénients de ces fonctions avant de les utiliser pour résoudre des problèmes mathématiques spécifiques.

D'abord, on a présenté l'essentiel, en terme de notions, de la théorie des fonctions génératrices. Ainsi, certaines types qui existent dans la literature. Ensuite, on a abordé des techniques de calcul dans la mesure où on arrive à obtenir des fonctions génératrices de certaines suites connues. On a terminé ce travail par donner certaines applications de ces fonctions en combinatoire : comment construire la formule explicite des coefficients binomiaux, en théorie des graphes : énumérer le nombre de certaine structure de graphe, en statistiques : calculer la probabilité d'extinction et en informatique : corriger des données transmises dus à des interférences de signal ou d'une mauvaise qualité de communication.

En résumé, les fonctions génératrices ont une large domaines d'applications et offrent des perspectives intéressantes pour résoudre des problèmes mathématiques et algorithmiques. Leur utilisation peut conduire à des méthodes plus efficaces pour résoudre des problèmes complexes dans différents domaines.

BIBLIOGRAPHIE

[1] K. Boubellouta, *Fonctions symétriques et leurs applications à certains nombres et polynômes* , Thèse, Université Mohamed Seddik Ben Yahia, Jijel, Algeria, (2020).

[2] N. Bouffard, *Combinatoire 1*, Université de saint-boniface, (1818).

[3] M. El amrani, *Suites et séries numériques : Suites et séries de fonctions* , Ellipses marketing, (2011).

[4] M. J. Erickson, *Introduction to combinatorics*, John wiley-Sons, (2013).

[5] D. Foata, G. Han, *Principe de combinatoire classique*, Cours, Université Louis Pasteur, (2008).

[6] P. Jolissaint, *Fonction génératrices et relations de récurrence*, Presses polytechniques et universitaires romandes, (2015).

[7] J. Harris, J. L. Hirst, M. J. Mossinghoff, *Combinatorics and graph theory*, Undergraduate texts in mathematics, (2008).

[8] H. Zerouk, *Fonctions génératrices de certains produits de nombres et polynômes*, Thèse, Université Mohamed Seddik Ben Yahia, Jijel, Algeria,(2022).

[9] W. Gould, *The Lagrange interpolation formula and Stirling numbers*, Proc. Amer. Math. Soc, 11 :421-425, (1960).

[10] W. Gould, *Stirling number representation problems*, Proc. Amer. Math. Soc., 11 :447-451. (1960).

[11] S. Lando, *Lectures on Generating Functions*, American mathematical society, 23(2003).

[12] N. Loehr, *Combinatorics*, second ed. Chapman and Hall/CRC, (2017).

[13] I. Mező, *Combinatorics and number theory of counting sequences*, CRC Press, (2019).

[14] J. Quatance, H. W. Gould, *Combinatorial identities for Stirling numbers : the unpublished notes of HW Gould*, World Scientific, (2015).

[15] L.Schwartz, *ALGÈBRE 3e ANNÉE : Cours et exercices avec solutions*, Dunod, (2003).

[16] Y. Velenik, *Probabilités et Statistique*, Université de genève, (2016).

[17] R. Stanley, *Enumerative Combinatorics* 1, Cambridge University Press (1997).

[18] H. S. Wilf. *generatinfunctionology*, Acadimic press, (1990).

Résumé:

Le travail présenté dans ce mémoire est consacré à l'étude des applications des fonctions génératrices dans les sciences appliquées. Tout d'abord, quelques notions élémentaires de séries formelles et de fonctions génératrices ordinaires et exponentielles avec des relations de récurrence sont données. Ensuite, nous avons introduit une théorie des opérations pour les séries génératrices, telles que l'addition, la multiplication, la composition, etc. Nous avons également présenté quelques fonctions bien connues : la suite de Fibonacci, les nombres de catalans, les partitions, etc. Enfin, nous avons choisi quelques domaines d'application pour voir comment ces fonctions génératrices interviennent en tant que solutions aux problèmes posés.

Mots-clés : Fonction génératrice, Série formelle, Fonction génératrice ordinaire, Fonction génératrice exponentielle, Coefficient binomial, Applications des fonctions génératrices.

ملخص:

تم تخصيص العمل المقدم في هذه المذكرة لدراسةتطبيقات توليد الدوال العلوم التطبيقية. في البداية قمنا بالتذكير ببعض المفاهيم الأولية للسلاسل و الدوال المولدة العادية و الأسية مرفقة بالعلاقات التكرارية. بعدها قدمنا عمليات خاصة بالسلاسل المولدة مثل: الجمع، الضرب التركيب...ألخ. وايضا بعض الدوال المعروفة: فيبوناشي، الاعداد الكاتالونية، التجزئة وغيرها. في الأخير استعنا ببعض التطبيقات لتوليد الدوال في العلوم التطبيقية.

الكلمات المفتاحية:الدوال المولدة، سلاسل، دوال التوليد العادية، دوال التوليد الأسية، معاملات ثنائية الحد .

.

Abstract

The work presented in this memoir is devoted to the study of applications of generating functions in the applied sciences. First, some elementary notions of formal series and ordinary and exponential generating functions with recurrence relations are given. Next, we introduce a theory of operations for generating series, such as addition, multiplication, composition, etc. We also introduced some well-known functions: the Fibonacci sequence, Catalan numbers, partitions, etc. Finally, we have chosen a few fields of application to see how these generating functions come into play as solutions to the problems posed.

Keywords: Generating function, Formal series, Ordinary generating function, Exponential generating function, Binomial coefficient, Applications of generating function.