Chapitre IV

Chapitre IV : Relations de récurrence



"I spoke to my old math teacher today. He says don't give up hope, someday algebra WILL be useful to me."

Question du jour

Quel est le point commun entre les lapins, les pommes de pins et le pavage par des rectangles ?



Dans ce premier exemple, nous étudions le problème suivant :

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

Définition 1 (Droites en position générale)

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

Appelons $\Phi_2(n)$ le nombre de régions du plan délimitées par n droites en position générale. Notre but est d'obtenir une formule close pour $\Phi_2(n)$.

En particulier, nous allons voir que *le nombre de régions dépend* uniquement du nombre de droites, et pas de l'arrangement lui-même. Comment procéder? Voyons tout d'abord ce que vaut $\Phi_2(n)$ pour des petites valeurs de n.







n=2

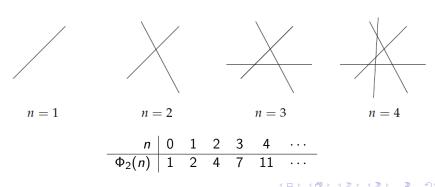


n = 3



n = 4

En particulier, nous allons voir que le nombre de régions dépend uniquement du nombre de droites, et pas de l'arrangement lui-même. Comment procéder? Voyons tout d'abord ce que vaut $\Phi_2(n)$ pour des petites valeurs de n.



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



Théorème 1

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

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

A choice

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

<u>Démonstration</u>:

Le fait que $\Phi_2(0)$ est bien défini et vaut 1 est évident.

Maintenant, supposons $n \ge 1$ et supposons $\Phi_2(n-1)$ bien défini. Numérotons les droites de l'arrangement D_1, \ldots, D_n . Le nombre de régions délimitées par les droites D_1, \ldots, D_{n-1} vaut $\Phi_2(n-1)$.

coupe certaines des régions de l'arrangement D_1, \ldots, D_{n-1} en deux. Le nombre de telles régions est égal au nombre d'intervalles de la droite D_n délimités par D_1, \ldots, D_{n-1} , c'est-à-dire n. Donc $\Phi_2(n)$ est bien défini et vaut $\Phi_2(n-1) + n$. \square

Rajoutons la droite D_n à cet arrangement. Cette dernière droite

$$\phi_1(n) = \oint_2(n-1) + n$$

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

$$\Phi_{2}(n) = n + \Phi_{2}(n-1)$$

$$= n + (n-1) + \Phi_{2}(n-2)$$

$$\vdots$$

$$= n + (n-1) + (n-2) + \dots + 1 + \Phi_{2}(0)$$

$$= \frac{n(n+1)}{2} + 1$$

$$= \frac{n(n+1)}{2} + n + 1$$

$$= \frac{n^{2} - n + 2n}{2}$$

$$= \binom{n}{2} + \binom{n}{1} + \binom{n}{0}$$

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

Definition 1 (Plans en position générale)

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

$$\phi_{3}(1) = \gamma$$

$$\phi_{3}(1) = \gamma + \gamma$$

$$\phi_{3}(1) \Rightarrow \phi_{2}(1)$$

Appelons $\Phi_3(n)$ le nombre de régions de l'espace délimitées par n plans (en position générale).

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

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

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

La dernière égalité utilise (trois fois) l'identité de somme parallèle (Théorème 25 du Chapitre 1)

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

$$\Phi_d(n) = \Phi_d(n-1) + \Phi_{d-1}(n-1) \quad \forall n \geqslant 1; \quad \Phi_d(0) = 1$$

et pour la formule :

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

Etudions maintenant le problème suivant :

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

Notons ce nombre p_n (pour $n \ge 0$).

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

- a) soit le rectangle dans le coin inférieur gauche est vertical;
- b) soit le rectangle dans le coin inférieur gauche est horizontal.

Dans le cas

- a) on peut compléter le pavage par n'importe quel pavage d'un rectangle $2 \times (n-1)$.
- b) le rectangle situé juste au-dessus est également horizontal et on peut compléter le pavage par n'importe quel pavage d'un rectangle $2 \times (n-2)$.

De plus, il est évident que $p_1 = 1$ et $p_2 = 2$. En résumé :

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

Pour les petites valeurs de n, on trouve :

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

Définition 2 (Suite de Fibonacci)

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

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

(certaines définitions démarrent la suite par $F_{1} = 1$, $F_{2} = 1$)

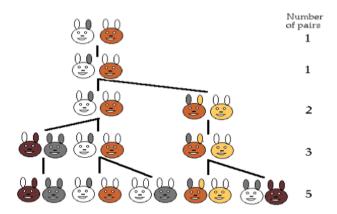
Leonardo Fibonacci





Liber Abaci (Book of Calculation) 1202

La question d'origine, les lapins de Fibonacci :



Exemple 2

Trouvez les quotients suivants : Que remarquez-vous?



1/1	
2/1	
3/2	
5/3	
8/5	
13/8	
21/13	
34/21	
55/34	
89/55	combre d'or
→ ^	munitar 9 oc

Comme les quotients deviennent de plus en plus grand quel nombre approche-t-on?

Exemple 3 (suite de l'exemple précédent)

$$\begin{array}{rcl} \frac{1}{1} & = & 1 \\ \\ \frac{2}{1} & = & \frac{1+1}{1} = 1 + \frac{1}{1} \\ \\ \frac{3}{2} & = & \frac{2+1}{2} = \frac{2}{2} + \frac{1}{2} = 1 + \frac{1}{\frac{2}{1}} = 1 + \frac{1}{1+\frac{1}{1}} \\ \\ \frac{5}{3} & = & \frac{3+2}{3} = \frac{3}{3} + \frac{2}{3} = 1 + \frac{1}{\frac{3}{2}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{2}}} \end{array}$$

Le Nombre d'Or :

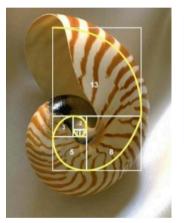
$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \cdots}}}$$

$$\varphi = 1 + \frac{1}{1 + \frac{1}{1 + \cdots}}$$

Le Nombre d'Or : Résoudre l'équation suivante pour φ .

$$\varphi = 1 + \frac{1}{\varphi}.$$

Le Nombre d'Or est partout!







Le Nombre d'Or est partout!



Nous allons maintenant trouver une formule explicite pour le n-ème nombre de Fibonacci F_n .

L'étudiant familier avec les méthodes de résolution d'équations différentielles linéaires à coefficients constants devrait facilement s'y retrouver car ces équations se résolvent de la même manière que les équations de récurrence linéaires à coefficients constants, comme par exemple celle qui définit la suite de Fibonacci.

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

remplaçant
$$P_n$$
 par β^n :
$$\beta^n = \beta^{n-1} + \beta^{n-2} \quad \forall n \ge 2$$

$$\beta^1 - \beta^{-1} \quad \iff \beta = \frac{1 \pm \sqrt{5}}{2}.$$

Définition 3 (Nombre d'or)

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

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

$$F_n = \lambda_1 \varphi^n + \lambda_2 \bar{\varphi}^n \quad \forall n \in \mathbb{N}$$
 (1)

est également solution, pour tout choix de constantes $\lambda_1, \lambda_2 \in \mathbb{R}$.

Ceci est dû au fait que l'ensemble des suites solutions de notre équation de récurrence forme un sous-espace vectoriel de l'espace vectoriel $\mathbb{R}^{\mathbb{N}}$ des suites réelles. \bigwedge \rightarrow \bigwedge

Or la dimension de ce sous-espace est *exactement* 2. Intuitivement, le choix des conditions initiales F_0 et F_1 donne deux degrés de liberté, et tout est déterminé quand on connaît F_0 et F_1 . Les suites $(\varphi^n)_{n\in\mathbb{N}}$ et $(\bar{\varphi}^n)_{n\in\mathbb{N}}$ étant linéairement indépendantes (voyez-vous pourquoi?), elles forment une *base* de l'espace des solutions. Dès lors, toute suite solution est de la forme (1).

Théorème 4

Pour tout $n \in \mathbb{N}$,

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

<u>Démonstration</u>:

Par ce qui précède, il existe des constantes $\lambda_1, \lambda_2 \in \mathbb{R}$ telles que F_n est donné par (1).

En imposant les conditions initiales $F_0 = 0$ et $F_1 = 1$, on trouve

$$n = 0: 0 = F_0 = \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right)^0 + \lambda_2 \left(\frac{1-\sqrt{5}}{2}\right)^0$$

$$n = 1: 1 = F_1 = \lambda_1 \left(\frac{1+\sqrt{5}}{2}\right)^1 + \lambda_2 \left(\frac{1-\sqrt{5}}{2}\right)^1.$$

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

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

En résolvant ce système, on trouve :

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

Remarque:

Etant donné que $\bar{\varphi}=-0,618\ldots$ est de valeur absolue strictement plus petite que 1, on a

$$\lim_{n\to\infty}\bar{\varphi}^n=0.$$

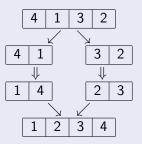
Donc, le *n*-ème nombre de Fibonacci F_n est simplement l'entier le plus proche de $\frac{1}{\sqrt{5}}\varphi^n$ (pour *n* suffisamment grand).

exemple d'algo "olivier pour rigner"

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

Exemple 5

Voyons un exemple pour N = 4.



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

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

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

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

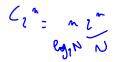
Après division par 2^n :

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

Après un moment de réflexion, on voit qu'il faut changer de variables et poser $a_n := \frac{C_2 n}{2^n}$. Résoudre la récurrence dans les nouvelles variables est un jeu d'enfant :

$$a_n = 1 + a_{n-1}$$
 $= 1 + 1 + a_{n-2}$
 $= \cdots$
 $= \underbrace{1 + 1 + 1 + 1 + \dots + 1}_{n \text{ fois}} + \underbrace{a_0}_{=0}$
 $= n$

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



Théorème 6

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

$$C_N = N \log_2 N$$
.

Récurrences linéaires

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

Récurrences linéaires du premier ordre



Théorème 7

La récurrence

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

a pour solution explicite

$$x_{n} = \sum_{i=1}^{n} d_{i} \prod_{j=i+1}^{n} c_{j} = \underbrace{d_{n} + d_{n-1}c_{n} + d_{n-2}c_{n-1}c_{n} + \cdots + d_{1}c_{2} \cdots c_{n}}_{\leftarrow}.$$

Remarque : Si $x_0 \neq 0$, alors on décale les indices des x_n, c_n, d_n jusqu'à obtenir $x_0 = 0$.

Récurrences linéaires du premier ordre

<u>Démonstration</u>: Par récurrence sur n. C'est vrai pour n = 0 (car une somme vide est par définition nulle). Supposons maintenant n > 0 et

typ unit pour
$$\left(x_{n-1} = \sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n-1} c_j.\right)$$

 $x_n = c_n x_{n-1} + d_n$

Alors

$$= c_n \sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n-1} c_j + d_n$$

$$= \sum_{i=1}^{n-1} d_i \prod_{j=i+1}^{n} c_j + d_n$$

$$= \sum_{i=1}^{n} d_i \prod_{j=i+1}^{n} c_j . \square$$

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

$$x_n = c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \cdots + c_0x_{n-d} \quad \forall n \geqslant d$$

ou encore

$$-x_n + c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \cdots + c_0x_{n-d} = 0 \quad \forall n \geqslant d . \quad (2)$$

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

Définition 4 (Polynôme caractéristique)

Le polynôme caractéristique de la RLCC (2) est

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

$$où c_d := -1.$$

Notre objectif est de comprendre l'ensemble des solutions des RLCC, c'est-à-dire l'ensemble des suites $(x_n)_{n\in\mathbb{N}}\in\mathbb{C}^\mathbb{N}$ qui satisfont (2). Nous verrons qu'il est possible d'écrire une formule close donnant toutes les solutions de (2).

Théorème 8

Notons S l'ensemble des solutions de la RLCC (2). Alors :

- (i) S est un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$,
- (ii) $\dim(S) = d$.

5 order de la recurrence

<u>Démonstration</u>: (Ne pas connaître pour l'examen)

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

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

satisfait, pour $n \geqslant d$:

$$z_{n} = \lambda x_{n} + \mu y_{n}$$

$$= \lambda (c_{d-1}x_{n-1} + \dots + c_{0}x_{n-d}) + \mu (c_{d-1}y_{n-1} + \dots + c_{0}y_{n-d})$$

$$= c_{d-1}(\lambda x_{n-1} + \mu y_{n-1}) + \dots + c_{0}(\lambda x_{n-d} + \mu y_{n-d})$$

$$= c_{d-1}z_{n-1} + \dots + c_{0}z_{n-d}.$$

L'ensemble des solutions est stable pour les combinaisons linéaires, c'est donc un sous-espace vectoriel de $\mathbb{C}^{\mathbb{N}}$.

(ii) Considérons l'application linéaire

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

Alors A est injective car le noyau $\ker(A) := \{x \in S \mid A(x) = 0\}$ de A est l'ensemble des suites solutions dont les d premières valeurs sont nulles. Par (2), la (d+1)-ème valeur d'une telle suite est également nulle, etc. . . Le noyau de A comporte donc une seule suite, la suite nulle. Ceci implique que A est injective car si $x = (x_n)_{n \in \mathbb{N}}$ et $y = (y_n)_{n \in \mathbb{N}}$ sont deux suites solution, alors

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

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

Définition 5 (Multiplicité)

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

i m=

Lemma 2

Soit $p(t) \in \mathbb{C}[t]$ un polynôme complexe de degré $d \geqslant 1$. Un nombre complexe a est une racine de multiplicité m = m(a) du polynôme p(t) si et seulement si

$$p(a) = \frac{\mathrm{d}p}{\mathrm{d}t}(a) = \cdots = \frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a) = 0 \text{ et } \frac{\mathrm{d}^mp}{\mathrm{d}t^m}(a) \neq 0.$$

<u>Démonstration</u>: (Ne pas connaître pour l'examen)

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

$$p(t) = p(a) + \frac{\mathrm{d}p}{\mathrm{d}t}(a)(t-a) + \frac{1}{2}\frac{\mathrm{d}^{2}p}{\mathrm{d}t^{2}}(a)(t-a)^{2} + \dots + \frac{1}{(m-1)!}\frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a)(t-a)^{m-1} + \frac{1}{m!}\frac{\mathrm{d}^{m}p}{\mathrm{d}t^{m}}(a)(t-a)^{m} + \dots + \frac{1}{d!}\frac{\mathrm{d}^{d}p}{\mathrm{d}t^{d}}(a)(t-a)^{d}.$$

Si
$$p(a) = \frac{\mathrm{d}p}{\mathrm{d}t}(a) = \cdots = \frac{\mathrm{d}^{m-1}p}{\mathrm{d}t^{m-1}}(a) = 0$$
 et $\frac{\mathrm{d}^mp}{\mathrm{d}t^m}(a) \neq 0$ alors clairement $p(t)$ est divisible par $(t-a)^m$ mais pas par $(t-a)^{m+1}$, donc a est une racine de multiplicité m .

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

Lemma 3

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

$$i^{j} = \alpha_{1} i + \alpha_{2} i(i-1) + \dots + \alpha_{j} i(i-1) \cdots (i-j+1)$$

$$= \sum_{k=1}^{j} \alpha_{k} i(i-1) \cdots (i-k+1) .$$

<u>Démonstration</u>: (Ne pas connaître pour l'examen)

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

$$i^{j} = \alpha_{1} i + \alpha_{2} i(i-1) + \dots + \alpha_{j} i(i-1) \dots (i-j+1)$$

$$= \sum_{k=1}^{j} \alpha_{k} i(i-1) \dots (i-k+1).$$

Alors

$$i^{j+1} = i \cdot i^{j}$$

$$= i \cdot (\alpha_{1} i + \alpha_{2} i(i-1) + \dots + \alpha_{j} i(i-1) \dots (i-j+1))$$

$$= \alpha_{1} i^{2} + \alpha_{2} i^{2}(i-1) + \dots + \alpha_{j} i^{2}(i-1) \dots (i-j+1)$$

$$= \alpha_{1} (i + i(i-1)) + \alpha_{2} (i + i(i-1))(i-1)$$

$$+ \dots + \alpha_{j} (i + i(i-1))(i-1) \dots (i-j+1)$$

$$= \sum_{k=1}^{j} \alpha_{k} i(i-1) \dots (i-k+1) + \alpha_{1} i(i-1)$$

$$+ \sum_{k=2}^{j} \alpha_{k} i(i-1)^{2} \dots (i-k+1)$$

On peut ensuite remplacer $(i-1)^2$ dans la dernière somme par (i-1)+(i-1)(i-2), etc. . .

En continuant le calcul, on obtient en définitive une expression de i^j comme combinaison linéaire à coefficients entiers de i, i(i-1), i(i-1)(i-2), ..., $i(i-1)\cdots(i-k)$. \square

Lemma 4

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

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

pour j ∈ {0, . . . , m − 1} et

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

<u>Démonstration</u>: (Ne pas connaître pour l'examen)

Par le Lemme 3, on a

$$\sum_{i=0}^{d} c_i i^j a^i = \sum_{i=0}^{d} c_i \left(\sum_{k=1}^{j} \alpha_k i(i-1) \cdots (i-k+1) \right) a^i$$

$$= \sum_{k=1}^{j} \alpha_k \left(\sum_{i=0}^{d} c_i i(i-1) \cdots (i-k+1) a^i \right)$$

$$= \sum_{k=1}^{j} \alpha_k p^{\underline{k}}(a) .$$

Par le Lemme 2, cette dernière expression est nulle quand j < m et non nulle quand j = m (notons qu'on a toujours $\alpha_j = 1$). \square

Théorème 9 (Récurrences linéaires homogènes à coefficients constants)

Considérons la RLCC homogène d'ordre $d\geqslant 1$:

inférieur à la multiplicité de β .

$$-x_n+c_{d-1}x_{n-1}+c_{d-2}x_{n-2}+\cdots+c_0x_{n-d}=0 \quad \forall n\geqslant d$$
 . Psymbol 0 où $c_0,\ldots,c_{d-1}\in\mathbb{C}$ et $c_0\neq 0$. Notons $p(t):=\sum_{i=0}^d c_it^i\in\mathbb{C}[t]$ son polynôme caractéristique, où $c_d:=-1$. Toute solution de cette relation de récurrence est une combinaison linéaire des d suites de la forme $(n^j\beta^n)_{n\in\mathbb{N}}$, où β est une racine de $p(t)$ et $j\in\{0,1,\ldots,m(\beta)-1\}$, $c.-\hat{a}-d$. j est un naturel strictement

<u>Démonstration</u>: (Ne pas connaître pour l'examen)

Soit S l'ensemble des suites solutions de l'équation. Par le Théorème 6, S est un espace vectoriel sur le corps des complexes, de dimension d. Considérons maintenant une racine β de p(t), de multiplicité $m=m(\beta)\geqslant 1$. Etant donné que $c_0\neq 0$, on a $\beta\neq 0$. La suite $(n^j\beta^n)_{n\in\mathbb{N}}$ est solution de l'équation si et seulement si, pour tout naturel $n\geqslant d$,

$$\sum_{i=0}^{d} c_i (i + (n-d))^j \beta^{i+(n-d)} = 0$$

$$\stackrel{\beta \neq 0}{\iff} \sum_{i=0}^{d} c_i (i + (n-d))^j \beta^i = 0$$

$$\iff \sum_{i=0}^{d} c_i \left(\sum_{k=0}^{j} {j \choose k} i^{j-k} (n-d)^k \right) \beta^i = 0$$

$$\iff \sum_{k=0}^{j} {j \choose k} (n-d)^k \left(\sum_{i=0}^{d} c_i i^{j-k} \beta^i \right) = 0.$$

Par le Lemme 3, $\sum_{i=0}^{d} c_i i^{j-k} \beta^i = 0$ dès que j < m. Donc en particulier on voit que la suite $(n^j \beta^n)_{n \in \mathbb{N}}$ est solution pour

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

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

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

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

digit?

Exemple 10

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

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

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

Exemple 11

Quelle est la solution de $x_n=5x_{n-1}-6x_{n-2}$ pour $n\geqslant 2$ avec $x_0=0$ et $x_1=1$?

$$x_n=3^n-2^n.$$

(3)
$$x_n = \lambda_1 3^n + \lambda_2 2^n$$

(4) $C_{\underline{I}} \begin{cases} x_0 = 0 \\ x_1 = 1 \end{cases}$ $0 = x_0 = \lambda_1 3^n + \lambda_2 2^n + \lambda_3 2^n + \lambda_4 2^n + \lambda_5 2^$

$$\begin{cases} 3 = \lambda_1 + \lambda_1 \\ 1 = 3\lambda_1 + 7 & \lambda_1 \end{cases} \begin{cases} \lambda_1 = -1 \\ \lambda_1 = 1 \\ \lambda_1 = 1 \end{cases}$$

$$(5) \text{ Sol. particulian}; \lambda_m = 3^m - 2^m$$

Récurrences linéaires à coefficients constants générales

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

$$-x_n + c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \dots + c_0x_{n-d} = a_n \quad \forall n \geqslant d$$

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

$$-x_n + c_{d-1}x_{n-1} + c_{d-2}x_{n-2} + \cdots + c_0x_{n-d} = 0 \quad \forall n \geqslant d.$$

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

Récurrences linéaires à coefficients constants générales

En d'autres termes, la solution générale de l'équation de départ $x_n = x_n^{EHA} + x_n^{SP} \quad \forall n \in \mathbb{N}$ s'exprime comme

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

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

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



"Really? — my people always say multiply and conquer."

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

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

$$C_N = C_{\lceil N/2 \rceil} + C_{\lfloor N/2 \rfloor} + N \quad \forall N \geqslant 2; \quad C_1 = 0$$
 est $C_N = N \lg N$. C'est un exemple de récurrence diviser-pour-régner ("divide-and-conquer"). Celles-ci sont

- très importantes en analyse d'algorithmes;
- sujettes à des comportements oscillatoires / fractals dûs à la présence de [...] et [...].

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

Récurrences diviser-pour-régner : Recherche binaire

Pour localiser un nombre x dans un vecteur trié de taille N, l'algorithme de **recherche binaire** compare x au $\lceil N/2 \rceil$ -ème élément du vecteur (appelé **pivot**).

- \blacksquare Si x est égal au pivot, l'algorithme s'arrête en ayant localisé x.
- Si x est plus petit que le pivot, l'algorithme s'appelle récursivement sur le sous-vecteur constitué des éléments en positions 1 jusque $\lceil N/2 \rceil 1$.
- Si x est plus grand que le pivot, l'algorithme s'appelle récursivement sur le sous-vecteur constitué des éléments en positions $\lceil N/2 \rceil + 1$ jusque N.

Récurrences diviser-pour-régner : Recherche binaire

Théorème 12

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

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

avec $B_1 = 1$.

Récurrences diviser-pour-régner : Recherche binaire

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

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

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

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

$$\textit{C}_{\textit{N}} = \textit{C}_{\lceil \textit{N}/2 \rceil} + \textit{C}_{\lfloor \textit{N}/2 \rfloor} + \textit{N} \quad \forall \textit{N} \geqslant 2; \quad \textit{C}_1 = 0 \ .$$

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

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

L'avant-dernière égalité résulte du fait que $\lceil (N+1)/2 \rceil = \lfloor N/2 \rfloor$ pour tout entier N.

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

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

$$C_{N} = C_{N} - 0$$

$$= C_{N} - C_{1}$$

$$= (C_{N} - C_{N-1}) + (C_{N-1} - C_{N-2}) + \dots + (C_{2} - C_{1})$$

$$= D_{N-1} + D_{N-2} + \dots + D_{1}$$

$$= \sum_{k=1}^{N-1} (\lfloor \lg k \rfloor + 2)$$

$$= (N-1) + \sum_{k=1}^{N-1} (\lfloor \lg k \rfloor + 1) .$$

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

Exemple 13

Par exemple, $C_9 = 8 + 21 = 29$ car le nombre total de bits écrits quand on écrit les représentations binaires de 1, 2, ..., 8 est exactement 21.

Théorème 14

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

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

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

Récurrences diviser-pour-régner : Retour au tri-fusion

Démonstration :

- Les nombres 1, ..., N-1 ont $\geqslant 1$ bit dans leur représentation binaire.
- Parmi ceux-ci, seuls les nombres 2, ..., N-1 ont $\geqslant 2$ bits dans leur représentation binaire.
- Parmi ceux-ci, seuls les nombres 4, ..., N-1 ont ≥ 3 bits dans leur représentation binaire.
- Etc...

On en déduit :

$$C_{N} = (N-1) + (N-1) + (N-2) + (N-4) + \dots + (N-2^{\lfloor \lg N \rfloor})$$

$$= (N-1) + (N-2^{0}) + (N-2^{1}) + (N-2^{2}) + \dots + (N-2^{\lfloor \lg N \rfloor})$$

$$= (N-1) + N(\lfloor \lg N \rfloor + 1) - (2^{0} + 2^{1} + 2^{2} + \dots + 2^{\lfloor \lg N \rfloor})$$

$$= N |\lg N| + 2N - 2^{\lfloor \lg N \rfloor + 1}. \quad \Box$$

Récurrences diviser-pour-régner : Rappels sur les comportements asymptotiques

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

- $f \sim g$ si $\lim_{n \to \infty} \frac{f(n)}{g(n)} = 1$, on dit alors que f et g sont asymptotiquement équivalentes;
- f = O(g) s'il existe une constante C > 0 et $n_0 \in \mathbb{N}$ tels que
- $f(n) \leqslant Cg(n)$ pour $n \geqslant n_0$; "dominate a particle of $f(n) \leqslant Cg(n)$ pour $f(n) \geqslant n_0$; "dominate a particle of $f(n) \geqslant n_0$, "dominate a partic

 - $f = \Theta(g)$ si f = O(g) et g = O(f), on dit alors que f et gont même comportement asymptotique.

Récurrences diviser-pour-régner : Rappels sur les comportements asymptotiques

Exemple 15

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

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

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

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

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

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

$$a_{N} = \alpha a_{N/\beta} + f(N) \quad \forall N \in \mathbb{N} ,$$
 (3)

où N/β doit être interpreté tantôt comme $\lfloor N/\beta \rfloor$, tantôt comme $\lceil N/\beta \rceil$.

La récurrence pour le tri fusion est un exemple où $\alpha=2$, $\beta=2$ et f(N)=N. La recherche binaire est un autre exemple, cette fois avec $\alpha=1$, $\beta=2$ et f(N)=1.

Pour commencer, étudions l'équation fonctionnelle :

$$a(x) = \alpha a(x/\beta) + x \quad \forall x > 1; \quad a(x) = 0 \quad \forall x \leqslant 1.$$
 (4)

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

Théorème 16

Si la fonction a : $\mathbb{R}_+ \to \mathbb{R}_+$ est une solution de (4), alors :

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

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

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

<u>Démonstration</u> (Ne pas connaître pour l'examen)

En déroulant, on trouve

$$a(x) = x + \alpha a(x/\beta)$$

$$= x + \frac{\alpha}{\beta} x + \alpha^2 a(x/\beta^2)$$

$$= \dots$$

$$= x \left(1 + \frac{\alpha}{\beta} + \frac{\alpha^2}{\beta^2} + \dots + \frac{\alpha^{t-1}}{\beta^{t-1}} \right)$$

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

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

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

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

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

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

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

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

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

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

Théorème 17 ("Master Theorem")

Soient $\alpha \geqslant 1$, $\beta > 1$ des constantes et $f : \mathbb{N} \to \mathbb{R}_+$ une fonction. Pour une suite $(a_N)_{N \in \mathbb{N}}$ solution de la récurrence diviser-pour-régner (3):

- Cas 1. Si $f(N) = O(N^{\log_{\beta} \alpha \varepsilon})$ pour $\varepsilon > 0$, alors $a_N = \Theta(N^{\log_{\beta} \alpha})$.
- Cas 2. Si $f(N) = \Theta(N^{\log_{\beta} \alpha})$, alors $a_N = \Theta(N^{\log_{\beta} \alpha} \log_2 N)$.
- Cas 3. Si $f(N) = \Omega(N^{\log_{\beta} \alpha + \varepsilon})$ pour $\varepsilon > 0$, et si $\alpha f(N/\beta) \leqslant Cf(N)$ pour une certaine constante C < 1 et N suffisamment grand, alors $a_N = \Theta(f(N))$.



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

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

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

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} . agenum{5}$$

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

L'algorithme classique calcule les n^2 coefficients c_{ij} en utilisant directement (5). Pour chaque coefficent c_{ij} , cet algorithme effectue n multiplications et n-1 additions. Au total, l'algorithme effectue $n^2 \cdot n = n^3$ multiplications et $n^2 \cdot (n-1) = n^3 - n^2$ additions. Ce qui fait un total de $2n^3 - n^2 = \Theta(n^3)$ opérations arithmétiques.

Cependant, il existe un algorithme qui fait (asymptotiquement) *mieux*, l'**algorithme de Strassen** (1969).

Pour n = 2, on a :

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

et l'algorithme classique calcule

$$c_{11} = a_{11}b_{11} + a_{12}b_{21}$$

$$c_{12} = a_{11}b_{12} + a_{12}b_{22}$$

$$c_{21} = a_{21}b_{11} + a_{22}b_{21}$$

$$c_{22} = a_{21}b_{12} + a_{22}b_{22}$$
.

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

Remarque:

Pour n = 2, le nombre total d'opérations arithmétiques ne diminue pas, mais *augmente*.

Cependant, nous verrons que le fait de pouvoir calculer le produit en seulement 7 multiplications va permettre, pour des valeurs de *n* plus grandes, de *diminuer* le nombre total d'opérations arithmétiques.

Strassen a observé qu'en calculant les 7 produits

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

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

$$c_{11} = I + II - IV + VI$$

 $c_{12} = IV + V$
 $c_{21} = VI + VII$
 $c_{22} = II - III + V - VII$

85 / 113

Exemple 18

$$IV + V = (a_{11} + a_{12}) \cdot b_{22} + a_{11} \cdot (b_{12} - b_{22})$$

$$= a_{11}b_{22} + a_{12}b_{22} + a_{11}b_{12} - a_{11}b_{22}$$

$$= a_{11}b_{12} + a_{12}b_{22}$$

$$= c_{12}.$$

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

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

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

De nouveau, on a (exercice) :

$$C_{11} = A_{11}B_{11} + A_{12}B_{21}$$

$$C_{12} = A_{11}B_{12} + A_{12}B_{22}$$

$$C_{21} = A_{21}B_{11} + A_{22}B_{21}$$

$$C_{22} = A_{21}B_{12} + A_{22}B_{22}$$

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

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

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

Pour trouver le comportement asymptotique de T(n), on utilise le "Master Theorem" avec $\alpha=7$, $\beta=2$ et $f(n)=18n^2$.

On commence par le calcul $\log_{\beta} \alpha = 2,81...>2$. Par conséquent,

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

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

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

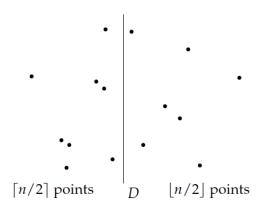
L'algorithme de Strassen est donc (asymptotiquement) meilleur que l'algorithme classique!

Remarque:

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

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

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

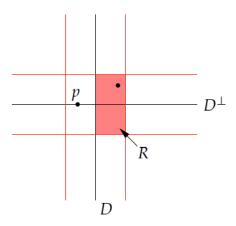


La figure illustre notre manière de diviser le problème : choisir une verticale D ne contenant aucun des n points et coupant le nuage de points en deux. Ceci semble être une bonne idée, mais comment recombiner?

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

Quelques observations:

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



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

Lemma 5

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

<u>Démonstration</u>:

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

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

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

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

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

Précalcul. Construire deux listes triées, l'une contenant l'ensemble des points triés par abscisses croissantes, et l'autre liste contenant l'ensemble des points triés par ordonnées croissantes. [⊖(n | g n)]

Partie récursive.

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

On trouve la récurrence diviser-pour-régner suivante :

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

qui a pour solution

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

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

Autres types de récurrences

Les types de récurrences vus jusqu'ici sont principalement :

- les récurrences linéaires à coefficients constants :
 - nombre de régions délimitées par *n* droites
 - **p** pavage d'un rectangle $2 \times n$
 - Fibonacci
- les récurrences diviser-pour-régner :
 - tri-fusion
 - recherche binaire
 - produit matriciel : Strassen
 - recherche de la plus proche paire

Nous terminons ce chapitre par deux exemples de récurrences d'autres types, chacun placé dans son contexte :

- calcul de la racine carrée
- fractions continuées

non cipiana on exposant

Considérons la récurrence suivante :

$$a_n = \frac{1}{2} \left(a_{n-1} + \frac{\beta}{a_{n-1}} \right) \quad n \ge 1; \quad a_0 = 1.$$
 (6)

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

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

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

et donc

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

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

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

$$b_n + \sqrt{\beta} = \frac{1}{2} \left(b_{n-1} + \sqrt{\beta} + \frac{\beta}{b_{n-1} + \sqrt{\beta}} \right)$$

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

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

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

Théorème 19

Pour tout $\beta > 0$, la solution $(a_n)_{n \in \mathbb{N}}$ de la récurrence (6) converge vers $\sqrt{\beta}$.

Démonstration :

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

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

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

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

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



Remarque:

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

$$b_n pprox rac{1}{2\sqrt{eta}}b_{n-1}^2$$

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

Exemple 20

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

n	a_n	$b_n = a_n - \sqrt{2}$
1	1,5	$0,0857\ldots < 10^{-1}$
2	1, <u>41</u> 666	$0,00245\ldots < 10^{-2}$
3	1, <u>4142</u> 1568	$0,000002123\ldots < 10^{-4}$
4	1, <u>41421356</u> 23	$\approx 2 \cdot 10^{-12} < 10^{-8}$
5	1, <u>414213562373</u>	$< 10^{-16}$

Fractions continuées

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

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

Aha! On dirait que les valeurs obtenues sont des quotients de nombres de Fibonacci consécutifs. (voir début du chapitre).

$$\lim_{n o\infty}a_n=rac{1}{1+rac{1}{1+rac{1}{1+rac{1}{1+\cdots}}}}$$

Fractions continuées

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

On sait (voir début du chapitre) que $a_n=rac{F_{n+1}}{F_{n+2}}$ et que $F_n\simrac{1}{\sqrt{5}}arphi^n$

Résumé des points importants du chapitre

- **1** exemples de récurrences : nombres de régions, pavages d'un rectangle, Fibonacci, Tri-fusion;
- 2 Récurrences linéaires du premier ordre;
- 3 Récurrences linéaires homogènes à coefficients constants;
- 4 Diviser pour régner : recherche binaire et tri-fusion ;
- Comportements asymptotiques et récurrences générales et Master Théorème;

Résumé des points importants du chapitre

- Application : Produit matriciel selon Strassen;
- Application : Recherche d'une plus proche paire ;
- 3 Autres types de récurrences : non-linéaire. Par exemple le calcul de la racine carrée et les fractions continuées (nombre d'or).