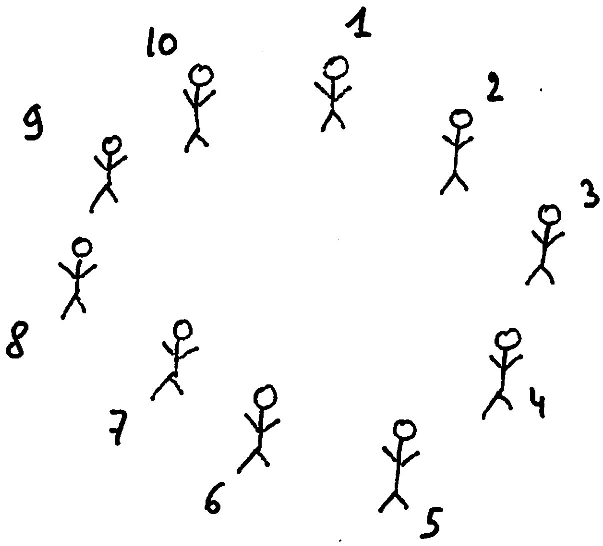
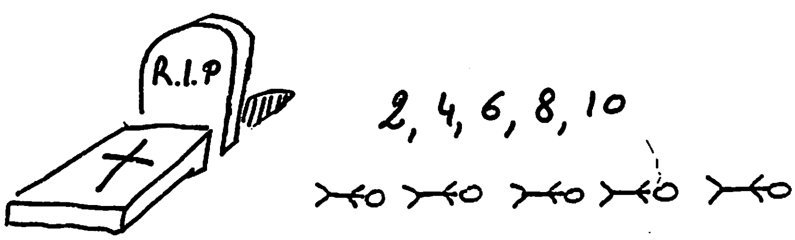
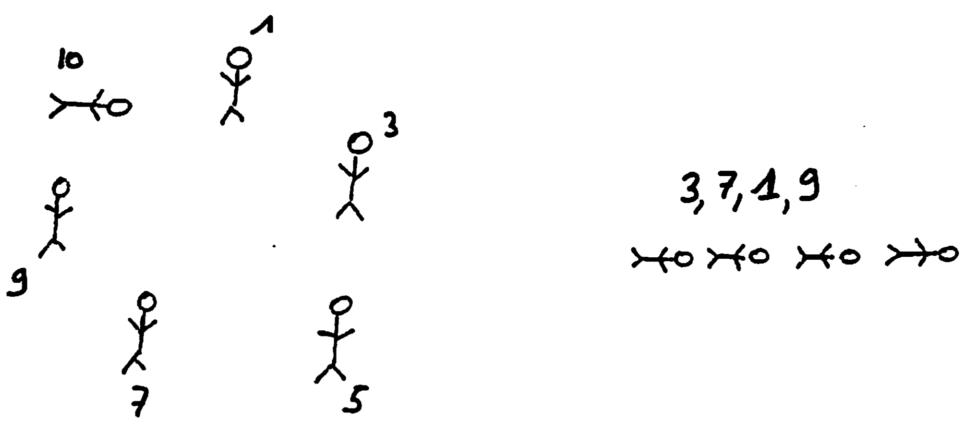
Suites Linéaires Récurrentes

Le problème de Josephus ...



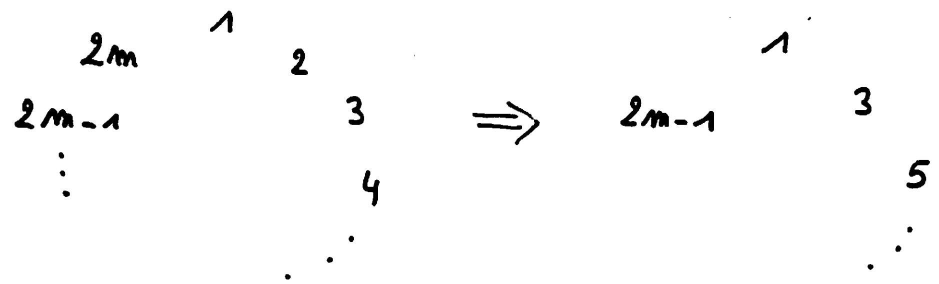




Josephus : $J(10) = 5$!

$$J(n) = ?$$

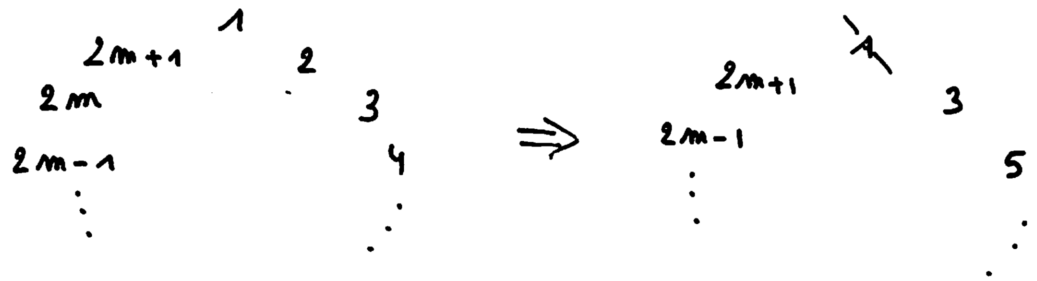
n pair



le prochain à être éliminé est le n° 3.

$$\boxed{J(2m) = 2\,J(m) - 1}$$

n impair



qd on élimine 1, on retrouve m personnes

$$\boxed{J(2m+1) = 2\,J(m) + 1}$$

$$\begin{cases} J(1) = 1 \\ J(2m) = 2\,J(m) - 1 \\ J(2m+1) = 2\,J(m) + 1 \end{cases}$$

Recherche d'une formule close

$$\begin{aligned} J(n) &= \sqrt{n^3 - 6n + 3} \\ &= \sin\left(\frac{n\pi}{2}\right) + \frac{n(n+1)}{2} \\ &= 2^n (n-1) + n\,3^n \\ &= \dots \end{aligned}$$

Inspection des premières valeurs de $J(n)$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$J(n)$	1	1	3	1	3	5	7	1	3	5	7	9	11	13	15	1
r	0	0	1	0	1	2	3	0	1	2	3	4	5	6	7	0

Si $\quad n = 2^m + r \quad$ avec $\quad 0 \leq r < 2^m$

$$\boxed{J(n) = 2r + 1}$$

<u>Preuve :</u> par récurrence sur m.

$m = 0$, alors $r = 0$, $n = 1$ et $J(n) = 1$ ok. ✓

induction : ok pour $m-1 \Rightarrow$ ok pour m ?

Si r est pair, $2^m + r$ est pair

$$J(2^m + r) = 2\, J\Big(\underbrace{\frac{2^m + r}{2}}_{2^{m-1} + \frac{r}{2}}\Big) - 1 \qquad \text{vu formule}$$

Vu hyp de réc.

$$= 2\left(2\,\frac{r}{2} + 1\right) - 1 = 2r + 1 \qquad ✓$$

Si r est impair, $2^m + r$ est impair

$$J(2^m + r) = 2\, J\Big(\underbrace{\frac{2^m + r - 1}{2}}_{2^{m-1} + \frac{r-1}{2}}\Big) + 1 \qquad \text{vu formule}$$

Vu hyp de réc.

$$= 2\Big(\underbrace{2\,\frac{r-1}{2}}_{r} + 1\Big) + 1 = 2r + 1 \qquad ✓$$

$n = 2^m + r$, $\quad J(n) = 2r+1$

<u>en base 2</u>

$$\rho_2(n) = \underbrace{x_m}_{x_m 2^m} + \underbrace{x_{m-1} \cdots x_1 x_0}_{r}$$

$x_i \in \{0,1\}$

$x_m = 1$

car $2^m \leq n < 2^{m+1}$

$$\rho_2(r) = x_{m-1} \cdots x_0 \Rightarrow \rho_2(2r) = x_{m-1} \cdots x_0 0$$

$$\rho_2(2r+1) = x_{m-1} \cdots x_0 1$$

$$= x_{m-1} \cdots x_0 x_m$$

donc $\quad \rho_2(n) = x_m x_{m-1} \cdots x_1 x_0$

$$\rho_2(J(n)) = x_{m-1} \cdots x_1 x_0 x_m$$

la suite $(J^k(n))_{k \in \mathbb{N}}$ se stabilise et on connaît la valeur.

$53 = 32 + 16 + 4 + 1$

53	1 1 0 1 0 1
$J(53)$	1 0 1 0 1 1
$J^2(53)$	$\cancel{0}$ 1 0 1 1 1
$J^3(53)$	$\cancel{0}$ 1 1 1 1
$J^4(53)$	1 1 1 1
	⋮

se stabilise

$1\,1\,0\,1\,\boxed{0}\,1$

3 "1"

après 3 étapes

et la valeur

$\underbrace{1 \cdots 1}_{t} \qquad 2^t - 1$

Version généralisée   construction d'un "répertoire"

$$\begin{cases} f(1) = \alpha \\ f(2n) = 2\, f(n) + \beta & n \geq 1 \\ f(2n+1) = 2\, f(n) + \gamma \end{cases}$$

n	$f(n)$	
1	α	0
2	$2\alpha + \beta$	0
3	$2\alpha + \gamma$	1
4	$4\alpha + 3\beta$	0
5	$4\alpha + 2\beta + \gamma$	1
6	$4\alpha + \beta + 2\gamma$	2
7	$4\alpha + 3\gamma$	3
8	$8\alpha + 7\beta$	0
9	$8\alpha + 6\beta + \gamma$	1
$\vdots$	$\vdots$	$\vdots$

$$f(n) = A(n)\,\alpha + B(n)\,\beta + C(n)\,\gamma$$

<u>Conjecture</u> :

si $n = 2^m + r$, $0 \leq r < 2^m$

$\boxed{A(n) = 2^m}$ $\boxed{B(n) = 2^m - r - 1}$ $\boxed{C(n) = r}$

on peut procéder par récurrence, <u>ou</u>...

① Si $\alpha = 1$, $\beta = \gamma = 0$

$f(1) = 1$, $f(2m) = 2\, f(m)$, $f(2m+1) = 2\, f(m)$

$\Rightarrow \quad f(m) = 2^m = \underbrace{2^m}_{A(n)} \cdot \alpha \qquad \boxed{A(n) = 2^m}$

② $\exists$ α, β, γ permettant de défini la fonction $f(n) = 1$?

$$\begin{cases} f(1) = \alpha \\ f(2m) = 2\, f(m) + \beta \\ f(2m+1) = 2\, f(m) + \gamma \end{cases} \qquad \begin{cases} 1 = \alpha \\ 1 = 2 \cdot 1 + \beta \\ 1 = 2 \cdot 1 + \gamma \end{cases}$$

$\alpha = 1$, $\beta = \gamma = -1$ définiment la fonction $f(n) = 1$

d'où $\boxed{1 = A(n) - B(m) - C(n)}$

③ $\exists$ α, β, γ permettant de défini $f(n) = n$?

$$\begin{cases} 1 = \alpha \\ 2m = 2\, m + \beta \\ 2m+1 = 2\, m + \gamma. \end{cases}$$

$\alpha = 1$, $\beta = 0$, $\gamma = 1$

d'où $\boxed{n = A(m) + C(m)}$

Conclusion :
$$\begin{cases} A(n) = 2^m \\ A(n) - B(n) - C(n) = 1 \\ A(n) + C(n) = n \end{cases} \quad \Rightarrow C(n) = n - 2^m = r$$

$$\Rightarrow B(m) = 2^m - r - 1$$

<u>DEF</u> : Si $(x_n)_{n\in\mathbb{N}}$ vérifie

$$x_{n+k} = a_{k-1}\, x_{n+k-1} + \dots + a_0\, x_n \ , \qquad (*)$$

alors on dit que $(x_n)_{n\in\mathbb{N}}$ satisfait une relation de récurrence linéaire homogène d'ordre k $(a_0 \neq 0)$

On se place sur un anneau commutatif $(A,+,\cdot)$

$A^{\mathbb{N}}$: ensemble des suites sur A est un A-module

$$x = (x_n)_{n\in\mathbb{N}} \ , \quad y = (y_n)_{n\in\mathbb{N}}$$

$$x+y = (x_n+y_n)_{n\in\mathbb{N}} \ , \quad a.x = (a x_n)_{n\in\mathbb{N}} \quad a\in A.$$

<u>Prop</u> : l'ensemble des suites de $A^{\mathbb{N}}$ vérifiant $(*)$ est un A-sous-module $\cong A^k$.

Preuve :

$$\underbrace{(x_0, \dots, x_{k-1})}_{\substack{k\text{-uple de} \\ \text{cond. initiales}}} \longleftrightarrow \text{une suite satisf. } (*)$$

$\left.\begin{array}{l} x = (x_n)_{n\in\mathbb{N}} \\ y = (y_n)_{n\in\mathbb{N}} \end{array}\right\}$ satisfaisant $(*)$

$$x_{n+k} + y_{n+k} = a_{k-1}(x_{n+k-1} + y_{n+k-1}) + \dots + a_0(x_n+y_n)$$

$$x_{n+k} = a_{k-1} x_{n+k-1} + \cdots + a_0 x_n$$

Polynôme caractéristique :

$$X^k - a_{k-1} X^{k-1} - \cdots - a_0 \in A[X], \text{ poly. de deg } k$$

Exemple : Fibonacci $\begin{cases} x_{n+2} = x_{n+1} + x_n, & \forall n \geq 0 \\ x_0 = 1, \; x_1 = 2. \end{cases}$

Pol. car. $X^2 - X - 1 = \left(X - \frac{1+\sqrt{5}}{2}\right)\left(X - \frac{1-\sqrt{5}}{2}\right)$

1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...

2, 4, 6, 10, 16, 26, 42, 68, 110, 178, ...

Le cas non homogène :

$$x_{n+k} = a_{k-1} x_{n+k-1} + \cdots + a_0 x_n + b \qquad (1)$$

Equation homogène associée

$$x_{n+k} = a_{k-1} x_{n+k-1} + \cdots + a_0 x_n \qquad (2)$$

Prop : $\mathcal{S}_{(1)} = \text{sol. part}_{(1)} + \mathcal{S}_{(2)}$ Pensez aux Equadif L.C.C.

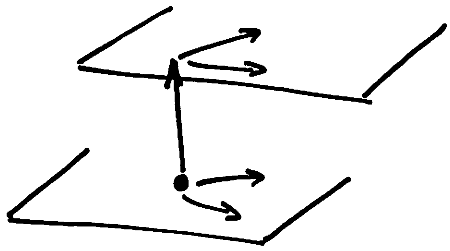
$\supset$ $(x_n)_{n\in\mathbb{N}} \in \mathcal{S}_{(1)}$, $(y_n)_{n\in\mathbb{N}} \in \mathcal{S}_{(2)}$

$$x_{n+k} + y_{n+k} = a_{k-1}(x_{n+k-1} + y_{n+k-1}) + \cdots + b$$

$\subset$ $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \mathcal{S}_{(1)}$

$$x_{n+k} - y_{n+k} = a_{k-1}(x_{n+k-1} - y_{n+k-1}) + \cdots + a_0(x_n - y_n)$$

Variété affine : Translaté d'un s.e.v



idem ici,
translaté d'1 A-n-module

1ère méthode de résolution : diagonalisation
et matrice compagnon

$$x_{n+k} = a_{k-1} x_{n+k-1} + \cdots + a_0 x_n$$

$$\mathcal{M} = \begin{pmatrix} a_{k-1} & a_{k-2} & \cdots & & a_0 \\ 1 & 0 & \cdots & & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} x_{n+k} \\ x_{n+k-1} \\ \vdots \\ x_{n+1} \end{pmatrix} = \mathcal{M} \begin{pmatrix} x_{n+k-1} \\ x_{n+k-2} \\ \vdots \\ x_n \end{pmatrix}$$

$$\begin{pmatrix} x_{n+k-1} \\ \vdots \\ x_n \end{pmatrix} = \mathcal{M}^n \begin{pmatrix} x_{k-1} \\ \vdots \\ x_0 \end{pmatrix}$$

exemple : Formule close pour Fibonacci

$$x_{n+2} = x_{n+1} + x_n$$

$$\begin{pmatrix} x_{n+1} \\ x_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \underbrace{\begin{pmatrix} x_1 \\ x_0 \end{pmatrix}}_{\begin{pmatrix} 2 \\ 1 \end{pmatrix}}$$

$$\tau = \frac{1+\sqrt{5}}{2}$$

$$\tau' = \frac{1-\sqrt{5}}{2}$$

$1^{\text{ère}}$ candi :

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \underbrace{\begin{pmatrix} \tau' & \tau \\ 1 & 1 \end{pmatrix}}_{S} \begin{pmatrix} \tau' & 0 \\ 0 & \tau \end{pmatrix} \underbrace{\frac{\sqrt{5}}{5}\begin{pmatrix} -1 & \tau \\ 1 & -\tau' \end{pmatrix}}_{S^{-1}}$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = S \begin{pmatrix} \tau'^n & 0 \\ 0 & \tau^n \end{pmatrix} S^{-1}$$

$$= \frac{\sqrt{5}}{5} \begin{pmatrix} \tau^{n+1} - \tau'^{n+1} & \tau^n - \tau'^n \\ \tau^n - \tau'^n & \tau\tau'^n - \tau'\tau^n \end{pmatrix}$$

$$x_n = \frac{\sqrt{5}}{5}(2-\tau')\,\tau^n + \frac{\sqrt{5}}{5}(\tau-2)\,\tau'^n$$

STRUCTURE DES SOLUTIONS

A anneau commutatif.

↳ on considère une extension convenable dans laquelle

$$\chi = X^k - a_{k-1}X^{k-1} - \dots - a_0 \quad \text{se factorise complètement}$$

$$\chi(X) = \prod_{j=1}^{r} (X - \alpha_j)^{m_j} \qquad m_1 + \dots + m_r = k$$

THM : $\chi = \prod_{j=1}^{r} (X-\alpha_j)^{m_j}$

$t < m_j$ $\qquad \left(n^t \alpha_j^n \right)_{n \in \mathbb{N}}$ est solution de l'ELRH.

COR :

$$\boxed{\sum_{j=1}^{r} T_j(n)\, \alpha_j^n \quad \text{où} \quad \deg T_j < m_j \quad \text{est solution de l'ELRH.}}$$

A quelles conditions cela constitue-t-il la solution générale de la récurrence ?

le pb vient de la multiplicité des racines d'un polynôme sur un anneau quelconque...

Rappel : Sur un champ de caractéristique nulle

α racine de P de mult. m ssi

$$P(\alpha) = \dots = (D^{m-1}P)(\alpha) = 0 \quad \text{et} \quad (D^m P)(\alpha) \neq 0$$

Ici, anneau commutatif intègre ce n'est exactement ça !

Ex : $\mathbb{Z}_3[X]$ $\qquad X^4 - X = X(X^3-1) = X(X-1)^3$

d'où 1 est racine triple

MAIS $\quad P(1) = 0$

$DP = 4X^3 - 1 = X^3 - 1, \quad (DP)(1) = 0$

$D^2P = 3X = 0, \quad (D^2P)(0) = 0$

$D^3P = 0$

$D^4P = 0$ $\qquad$ Toutes les dérivées sont nulles

$\vdots$

Ce que l'on peut dire :

1) <u>Lemme</u> : Si $\alpha \in A$ est racine de mult $\geq m$ de P

Alors $P(\alpha) = \dots = (D^{m-1}P)(\alpha) = 0$.

<u>Preuve</u> : $P(X) = (X-\alpha)^m \, Q(X)$

$i < m$ $\quad D^i P = \sum_{k=0}^{i} C_i^k \underbrace{D^k (X-\alpha)^m}_{\substack{\| \\ m(m-1)\cdots(m-k+1)\,(X-\alpha)^{\overbrace{m-k}^{>0}}}} D^{i-k}$

car $k \leq i < m$

$(D^i P)(\alpha) = 0$

2) <u>Prop</u> : A anneau commutatif intègre

$\boxed{m < \mathrm{car}(A)}$

α est racine de mult. $\geq m+1$

ssi $P(\alpha) = \dots = (D^m P)(\alpha) = 0$

<u>Preuve</u> : $\Rightarrow$ ok vu lemme.

$\Leftarrow$ Réc. sur m.

1) $m = 0$, $P(\alpha) = 0$, α racine de mult ≥ 1 ok !

2) ok pour $m-1$, ok pour m ?

$$\underbrace{P(\alpha) = \dots = (D^{m-1}P)(\alpha)}_{\text{on peut appliquer l'hyp de réc.}} = (D^m P)(\alpha) = 0$$

α est de mult. $\geq m$

$$P(X) = (X-\alpha)^m \, Q(X)$$

$$D^m P = \sum_{k=0}^{m} C_m^k \underbrace{D^k (X-\alpha)^m}_{\frac{m!}{(m-k)!}(X-\alpha)^{m-k}} D^{m-k} Q$$

$(X-\alpha)^{m-k}$ si $k<m$ $=0$ en α.

Par hyp, $(D^m P)(\alpha) = 0 = m! \, Q(\alpha)$

A intègre donc $m! = 0$ ou $Q(\alpha) = 0$

$$m! = \underbrace{1}_{\neq 0} . \underbrace{2}_{\neq 0} . \underbrace{3} \cdots \underbrace{m}_{\neq 0} \qquad m < \operatorname{car}(A)$$

la seule façon que $m! = 0$ c'est que $m!$ soit multiple de car A. Or car A est premier

$\Rightarrow m! \neq 0$

Donc $Q(\alpha) = 0$

$Q = (X-\alpha) R$

$P = (X-\alpha)^{m+1} R$ ok !

■

<u>Dém du thm</u> : $\left(n^t \alpha_j^n\right)_{n\in\mathbb{N}}$ solution de l'ELRH
$t < m_j$

<u>Thèse</u> : $$(n+k)^t \alpha_j^{n+k} = \sum_{i=0}^{k-1} a_i (n+i)^t \alpha_j^{n+i}$$

1)

$s \in \mathbb{N}$, $\quad P_s(X) := X(X-1)\ldots(X-s+1)$

polynôme de deg. s s'annulant en $0, 1, \ldots, s-1$

Rem : $\quad P_s(k) = \dfrac{k!}{(k-s)!}$

$\underset{\overset{\shortparallel}{1}}{P_0}, P_1, \ldots, P_t$ base des polynômes de deg $\leq t$

donc $$(X+n)^t = \sum_{\ell=0}^{t} c_\ell \, P_\ell(X)$$

2)

$$\chi(X) = X^k - a_{k-1}X^{k-1} - \ldots - a_0 = X^k - \sum_{i=0}^{k-1} a_i X^i$$

$(D^\ell \chi)(\alpha_j) = 0 \quad , \quad 0 \leq \ell \leq t \qquad$ car $\chi = \prod_{j=1}^{r} (X-\alpha_j)^{m_j}$

$$D^\ell \chi = \underbrace{\frac{k!}{(k-\ell)!}}_{P_\ell(k)} X^{k-\ell} - \sum_{i=\ell}^{k-1} a_i \underbrace{\frac{i!}{(i-\ell)!}}_{P_\ell(i)} X^{i-\ell}$$

$$(D^\ell \chi)(\alpha_j) = 0 = P_\ell(k)\,\alpha_j^{k-\ell} - \sum_{i=\ell}^{k-1} a_i \, P_\ell(i)\,\alpha_j^{i-\ell}$$

$$\Rightarrow \quad P_\ell(k)\, \alpha_j^{k-\ell} = \sum_{i=\ell}^{k-1} a_i\, P_\ell(i)\, \alpha_j^{i-\ell}$$

$\times\, \alpha_j^\ell$ $\downarrow$ $\qquad \ell \to 0$ car $P_\ell(i) = 0$ si $i < \ell$

$$P_\ell(k)\, \alpha_j^k = \sum_{i=0}^{k-1} a_i\, P_\ell(i)\, \alpha_j^i$$

$$\underbrace{(n+k)^t \alpha_j^{n+k}}_{\text{Vu 1)}} = \sum_{\ell=0}^{t} c_\ell\, \underbrace{P_\ell(k)}\, \underbrace{\alpha_j}^{n+\underbrace{k}}$$

$$= \sum_{\ell=0}^{t} c_\ell\, \alpha_j^n \sum_{i=0}^{k-1} a_i\, P_\ell(i)\, \alpha_j^i$$

$$= \sum_{i=0}^{k-1} a_i \underbrace{\left(\sum_{\ell=0}^{t} c_\ell\, P_\ell(i) \right)}_{(n+i)^t \text{ vu 1)}} \alpha_j^{n+i} \qquad \blacksquare$$

$$\chi = \prod_{j=1}^{r} (X - \alpha_j)^{m_j}$$

$m_1 \qquad (\alpha_1^n)_{n\in\mathbb{N}},\ (n\,\alpha_1^n)_{n\in\mathbb{N}},\ \dots,\ (n^{m_1-1}\alpha_1^n)_{n\in\mathbb{N}}$

$\vdots \qquad \vdots$

$m_r \qquad (\alpha_r^n)_{n\in\mathbb{N}},\ (n\,\alpha_r^n)_{n\in\mathbb{N}},\ \dots,\ (n^{m_r-1}\alpha_r^n)_{n\in\mathbb{N}}$

---

k

On a k solutions et l'ensemble des solutions est de dim. k ...

Calcul matriciel sur un anneau A

$\pm$ comme en $1^{ère}$ candi !

M inversible $\iff$ $\det M$ inversible ds A.

<u>Thm:</u> $\mathcal{M} = (c_1 \cdots c_n) \in A^n_n$

les cond. suivantes sont équivalentes :

1) $c_1, \dots, c_n$ engendrent A^n

2) ——— base de A^n

3) $\mathcal{M}$ est inversible

Si De plus, A est fini

4) $c_1, \dots, c_n$ sont lin. ind.

<u>Preuve</u> : 2) $\Rightarrow$ 1)

3) $\Rightarrow$ 2) $\mathcal{M}\mathcal{N} = I$

$$\sum_{k=1}^{n} [c_k]_i \, \mathcal{N}_{k,j} = \delta_{i,j} \quad \text{ou} \quad \sum_{k=1}^{n} \mathcal{N}_{k,j} \, [c_k]_i = [e_j]_i$$

càd $\displaystyle\sum_{k=1}^{n} \mathcal{N}_{k,j} \, c_k = e_i$

Engendrent A^n

partie libre ? $\displaystyle\sum_{i=1}^{n} \lambda_i c_i = 0$ et supposons $\lambda_1 \neq 0$

A anneau, λ_i pas néc^t^ inversible

$$\lambda_1 c_1 = - \sum_{i=2}^{n} \lambda_i c_i$$

$$\Rightarrow \det(\lambda_1 c_1 \; c_2 \cdots c_n) = 0 = \lambda_1 \underbrace{\det \mathcal{M}}_{\text{inversible}}$$

$\Rightarrow \lambda_1 = 0$.

1) $\Rightarrow$ 3)

$c_1, \dots, c_n$ engendent A^n donc en particulier e_j

$\exists \mathcal{N}_{k,j}$: $\sum_{k=1}^{n} \mathcal{N}_{k,j} \, c_k = e_j$

$$\sum_{k=1}^{n} \mathcal{N}_{k,j} \, [c_k]_i = [e_j]_i = \delta_{i,j}$$

$$\sum_{k=1}^{n} \mathcal{M}_{i,k} \, \mathcal{N}_{k,j} = \delta_{i,j}$$ d'où $\mathcal{M}$ est inversible.

A fini

3) $\Rightarrow$ 4) car 3) $\Rightarrow$ 2) (base donc lin. indép.)

4) $\Rightarrow$ 1)

a) $\rangle c_1, \dots, c_n \langle \subset A^n$

b) Si $(\lambda_1, \dots, \lambda_n) \neq (\lambda'_1, \dots, \lambda'_n)$ alors $\sum_i \lambda_i c_i \neq \sum_i \lambda'_i c_i$

car $c_1, \dots, c_n$ lin. indep.

donc $f : A^n \to \rangle c_1, \dots, c_n \langle : (\lambda_1, \dots, \lambda_n) \mapsto \sum_i \lambda_i c_i$

est une bijection

Puisque A est fini, $\# A^n = \# \rangle c_1, \dots, c_n \langle$

Vu a)

$$A^n = \rangle c_1, \dots, c_n \langle$$

Récapitulatif :

1) l'ensemble des solutions $\mathcal{S} \cong A^k$

2) $(n^t \alpha_j^n)_{n\in\mathbb{N}}$ $t<m_j$ sont k solutions de $\mathcal{S}$

d'où on regarde les cond initiales corresp.

$$\begin{array}{ccccccccc}
1 & 0 & & 0 & & 1 & & 0 \\
\alpha_1 & \alpha_1 & & \alpha_1 & & \alpha_r & & \alpha_r \\
\alpha_1^2 & 2\alpha_1^2 & \cdots & 2^{m_1-1}\alpha_1^2 & \cdots & \alpha_r^2 & \cdots & 2^{m_r-1}\alpha_r^2 \\
\vdots & \vdots & & \vdots & & \vdots & & \vdots \\
\alpha_1^{k-1} & (k-1)\alpha_1^{k-1} & & (k-1)^{m_1-1}\alpha_1^{k-1} & & \alpha_r^{k-1} & & (k-1)^{m_r-1}\alpha_r^{k-1}
\end{array}$$

3) Vu le thm précédent, engendrent A^k

si $\det\left(n^t \alpha_j^n\right)_{\substack{n=0,\dots,k-1 \\ j=1,\dots,r\ ;\ t=0,\dots,m_j-1}}$ inversible ds A

$$\| $$

$$\prod_{i=1}^{r} 0!\,1!\dots(m_i-1)!\ \alpha_i^{m_i(m_i-1)/2} \prod_{i<j}(\alpha_i-\alpha_j)^{m_i m_j}$$

On a donc la solution générale si

$$\begin{cases}
1)\ 1,2,\dots,(\sup m_i)-1 \text{ premier avec } \operatorname{car}(A) \\
2)\ \text{si } m_i \geq 2,\ \alpha_i \text{ est inversible dans } A \\
3)\ \forall i<j,\ \alpha_i-\alpha_j \text{ est inversible dans } A
\end{cases}$$

SUR $\mathbb{R}$ OU $\mathbb{C}$ TJS ok !

$\vec{x}_0, \vec{x}_1, \dots, \vec{x}_{q^k}$ $\quad q^k+1$ k-uple de $\mathbb{F}_q^k$

donc forcément 2 égaux !

$$\vec{x}_m = \vec{x}_n \qquad 0 \leq m < n \leq q^k$$

$$\vec{x}_n = M^{n-m} \vec{x}_m$$

On doit prouver la périodicité depuis x_ℓ

1^a cas $\quad a_0 \neq 0 \Longleftrightarrow \ell = 0$

$$M = \left(\begin{array}{ccc|c} a_{k-1} & \cdots & & a_0 \\ \hline 1 & & & 0 \\ & \ddots & & \vdots \\ & & 1 & 0 \end{array}\right)$$

$\det M = a_0 \neq 0$

donc M inversible

$$M^m \vec{x}_0 = \vec{x}_m = \vec{x}_n = M^n \vec{x}_0$$

M^{-m}

$$\boxed{\vec{x}_0 = M^{n-m} \vec{x}_0}$$

périodicité depuis x_0

2^e cas $\quad a_0 = \cdots = a_{\ell-1} = 0, \quad a_\ell \neq 0$

$$\underbrace{x_0, x_1, \dots, x_{\ell-1}}_{\text{ne jouent aucun rôle !}} \;\vdots\; x_\ell, x_{\ell+1}, \dots$$

$$y_0, y_1, \dots$$

$$y_n = x_{n+\ell}$$

Pour la suite y_n, on a

$$y_{n+(k-l)} = \sum_{i=0}^{k-l-1} a_{i+l}\, y_{n+i}$$

on s'est ramené au 1er cas, $(y_n)_{n\in\mathbb{N}}$ est périodique à partir de y_0, période $\leq q^{k-l}$

points 3 et 4)

e ordre de $\mathcal{M}$ dans $GL_k(\mathbb{F}_q)$: $\mathcal{M}^e = I$

donc $\mathcal{M}^e \vec{x}_0 = \vec{x}_0$

donc la période est $\boxed{\leq e}$

pour démontrer les 2 points, il suffit de vérifier que pour $x_0 = \cdots = x_{k-2} = 0$ et $x_{k-1} = 1$,

la période correspondante est $\boxed{\geq e}$

$$\vec{X}_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \qquad \underbrace{\mathcal{M}\vec{X}_0}_{\vec{X}_1} = \begin{pmatrix} * \\ 1 \\ 0 \\ | \\ 0 \end{pmatrix} \qquad \underbrace{\mathcal{M}^2\vec{X}_0}_{\vec{X}_2} = \begin{pmatrix} * \\ * \\ 1 \\ 0 \\ | \\ 0 \end{pmatrix}, \cdots$$

Rappel :

$$\mathcal{M} = \left(\begin{array}{ccc|c} a_{k-1} & \cdots & & a_0 \\ \hline 1 & & 0 & 0 \\ & \ddots & & \vdots \\ 0 & & 1 & 0 \end{array}\right)$$

$$\mathcal{A} = \left(\vec{X_0} \quad \vec{X_1} \quad \cdots \quad \vec{X_{k-1}} \right)$$

$$= \begin{pmatrix} 1 & * & * & & * \\ & 1 & * & & \vdots \\ & & 1 & & \vdots \\ & & & \ddots & * \\ & & & & 1 \end{pmatrix}$$

$\det \mathcal{A} = 1$
donc $\mathcal{A}$ inversible

$$\mathcal{M}^n \mathcal{A} = \left(\vec{X_n} \quad \vec{X_{n+1}} \quad \cdots \quad \vec{X_{n+k-1}} \right)$$

Si n est une période :

$$\mathcal{M}^n \mathcal{A} = \mathcal{A}$$

donc $\mathcal{M}^n = I$

donc n est un multiple de l'ordre de $\mathcal{M}$

$$\boxed{n \geq e}$$

$\blacksquare$

__Rem__ : on peut m̂ dire que la période est $\leq q^{k-\ell} \underbrace{-1}_{(0,\dots,0)}$

Un peu de cryptographie...

Chiffrement par flot

$\mathbb{Z}_2 = \mathbb{F}_2$

$$x_{n+4} = x_{n+1} + x_n \mod 2$$

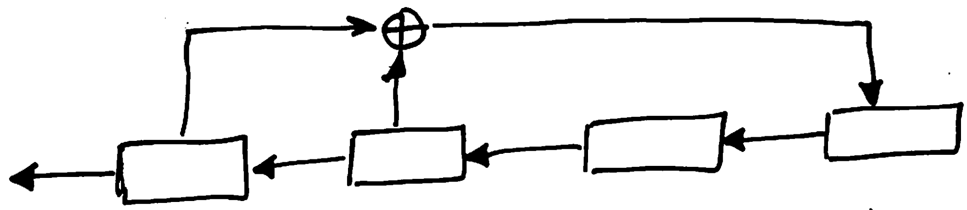
$x_0 = 0,\ x_1 = 0,\ x_2 = 0,\ x_3 = 1$

$\underline{0\ 0\ 0\ 1},\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1,\ \underline{0\ 0\ 0\ 1},$

$k = 4$
$\ell = 0$
$q = 2$

période $q^{k-\ell} - 1 = 2^4 - 1 = 15$

En pratique registre à décalage linéaire :



	x_0	x_1	x_2	x_3
x_0	x_1	x_2	x_3	$x_0 + x_1 = x_4$
x_1	x_2	x_3	x_4	$x_1 + x_2 = x_5$
$\vdots$				$\vdots$

texte	0	0	1	0	1	0	...
clé	0	0	1	0	0	1	...
	0	0	0	0	1	1	

La clé devrait paraître "aléatoire" à Oscar

<u>DANGER</u> : Si Oscar connaît k
et $2k$ élts de la suite lin. réc.

$$x_{l+1}, x_{l+2}, \dots, x_{l+2k} \quad \text{connus}$$

$$\underbrace{x_{l+1} - x_{l+k+1}}_{\text{connu}} = \sum_{i=0}^{k-1} a_i \, x_{l-k+i+1} - \sum_{i=0}^{k-1} a_i \, x_{l+i+1}$$

$$= \sum_{i=0}^{k-1} a_i \left(\underbrace{x_{l-k+i+1} - x_{l+i+1}}_{\text{connu}} \right)$$

$$x_{l+2} - x_{l+k+2} = \dots$$

$$\vdots$$

$$x_{l+k} - x_{l+2k} = \dots$$

Système de k éq. à k inconnues
$\Rightarrow a_0, \dots, a_{k-1}$ connus !
Prédictibilité.

<u>Rem</u> : Un autre générateur

$$\gamma \in \mathbb{Z}_p^*, \quad x_0 \in \mathbb{Z}_p^*, \qquad x_{n+1} = \gamma^{x_n} \bmod p$$

$$z_n = \begin{cases} 1 & \text{si } x_n > p/2 \\ 0 & \text{sinon} \end{cases}$$

prédictibilité $\Longleftrightarrow$ log. discret

Jusqu'à présent : - matrice compagnon
- factoriser χ

Autre méthode :

SÉRIES FORMELLES et GÉNÉRATRICES

A anneau

$A[z]$ anneau des polynômes

$$(a_0, a_1, \dots, a_k, 0, 0, \dots) \longleftrightarrow a_0 + a_1 z + \dots + a_k z^k$$

$A[[z]]$ anneau des séries formelles

$$(a_n)_{n \in \mathbb{N}} \longleftrightarrow \underbrace{\sum_{n=0}^{\infty} a_n z^n}$$

NOTATION Symbolique !
pas de notion de
convergence, etc ...

c'est juste un MOYEN COMMODE de
représenter une suite de $A^{\mathbb{N}}$.

$A[[z]]$ anneau :

$+$: $(a_n)_{n \in \mathbb{N}}$
$(b_n)_{n \in \mathbb{N}}$
$(a_n + b_n)_{n \in \mathbb{N}}$

$$\sum_{n=0}^{\infty} a_n z^n + \sum_{n=0}^{\infty} b_n z^n = \sum_{n=0}^{\infty} (a_n + b_n) z^n$$

• produit de Cauchy (ou de convolution)

$(a_n)_{n\in\mathbb{N}}$

$(b_n)_{n\in\mathbb{N}}$

$$\sum_{n=0}^{\infty} a_n z^n \cdot \sum_{n=0}^{n} b_n z^n$$

$$\shortparallel$$

$$\Big(\sum_{i+j=n} a_i b_j\Big)_{n\in\mathbb{N}} \qquad \sum_{n=0}^{\infty}\Big(\sum_{i+j=n} a_i b_j\Big) z^n$$

$$(a_0 + a_1 z + a_2 z^2 + \cdots)(b_0 + b_1 z + b_2 z^2 + \cdots)$$

$$= a_0 b_0 + (a_0 b_1 + b_0 a_1) z + (a_0 b_2 + a_1 b_1 + b_0 a_2) z^2 + \cdots$$

A est plongé ds $A[[z]]$: $a \mapsto a + 0z + 0z^2 + \cdots$

$A[z]$ ——————— : $a_0 + \cdots + a_n z^n$

$$\downarrow$$

$$a_0 + \cdots + a_n z^n + 0 z^{n+1} + \cdots$$

fonction génératrice d'une suite $(a_n)_{n\in\mathbb{N}}$

$$f_a(z) = \sum_{n=0}^{\infty} a_n z^n$$

$\boxed{A = \mathbb{R}}$

Une fraction rationnelle est un moyen compact pour représenter certaines fonctions gén

Ex: $\frac{1}{1-z}$ on procède par longue division

$$\begin{array}{l|l} 1 & 1-z \\ \cline{2-2} -(1-z) & 1+z+z^2+\cdots \\ \hline \quad z & \\ \quad -(z-z^2) & \\ \hline \qquad z^2 & \\ \qquad -(z^2-z^3) & \\ \hline \qquad\quad z^3 & \\ \qquad\qquad \ddots & \end{array}$$

Ainsi, $\frac{1}{1-z} = \sum_{n=0}^{\infty} 1 . z^n$ fonction gen. de la suite $(1)_{n\in\mathbb{N}}$

Vérif. $(1-z)(1+z+z^2+\cdots) = 1 + \underbrace{z-z}_{0} + \underbrace{z^2-z^2}_{0} + \cdots$

Ex : $\frac{z+z^2}{1-3z+3z^2-z^3} = \sum_{n=0}^{\infty} n^2 z^n$

$$\begin{array}{l|l} z+z^2 & 1-3z+3z^2-z^3 \\ \cline{2-2} \quad\vdots & z+4z^2+9z^3+\cdots \end{array}$$

OPÉRATIONS SUR LES SÉRIES :

- $\alpha\, s_a(z) + \beta\, s_b(z) = \sum_{n=0}^{\infty} (\alpha a_n + \beta b_n)\, z^n$

- $z^m s_a(z) = 0 + \cdots + 0 + \sum_{n=0}^{\infty} a_n z^{n+m}$

  série gén. de $\underbrace{0, 0, \ldots, 0}_{m}, a_0, a_1, \ldots$

- $$\frac{s_a(z) - a_0 - \cdots - a_{k-1} z^{k-1}}{z^k} = \sum_{n=0}^{\infty} a_{n+k}\, z^n$$

  série gén de $a_k, a_{k+1}, \ldots$

- Dérivation formelle

  $$D \sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} (n+1)\, a_{n+1}\, z^n$$

- Intégration formelle

  $$\int_0^z s_a(t)\, dt = a_0 z + \frac{1}{2} a_1 z^2 + \cdots = \sum_{n=1}^{\infty} \frac{1}{n} a_{n-1} z^n$$

▶ Suite des sommes partielles :

$$\underbrace{\frac{1}{1-z}}\ \underbrace{s_a(z)}$$

$$(1+z+z^2+z^3+\dots)\ (a_0+a_1 z+ a_2 z^2+\dots)$$

$$= a_0 + (a_0+a_1) z + (a_0+a_1+a_2) z^2 + \dots = \sum_{n=0}^{\infty} \left(\sum_{k=0}^{n} a_k\right) z$$

▶ Suite des termes d'indice pair
impair

$$\frac{s_a(z) + s_a(-z)}{2} = \frac{a_0+a_1 z+a_2 z^2+\dots + a_0 - a_1 z + a_2 z^2+\dots}{2}$$

$$= \sum_{n=0}^{\infty} a_{2n} z^{2n}$$

série gén. de $(a_0, 0, a_2, 0, a_4, 0, \dots)$

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

$(0, a_1, 0, a_3, 0, a_5, \dots)$

Exemple : Série génératrice de $(n^2)_{n\in\mathbb{N}}$

$$\frac{1}{1-z} = 1 + z + z^2 + z^3 + \cdots$$

D

$$\frac{1}{(1-z)^2} = 1 + 2z + 3z^2 + \cdots = \sum_{n=0}^{\infty} (n+1)\, z^n$$

$\cdot z$

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

D

$$\frac{1+z}{(1-z)^3} = \sum_{n=0}^{\infty} (n+1)^2\, z^n$$

$\cdot z$

$$\frac{z+z^2}{(1-z)^3} = \sum_{n=0}^{\infty} n^2\, z^n$$

on a donc la justification sans faire la longue division.

Les séries formelles sont utilisées pour résoudre des éq. de récurrence lin.

$$\sum_{n=0}^{\infty} a_n z^n = \sum_{n=0}^{\infty} b_n z^n \iff (a_n)_{n\in\mathbb{N}} = (b_n)_{n\in\mathbb{N}}$$

Expliquons la méthode sur un exemple ...

$$\begin{cases} x_{n+2} = x_{n+1} + x_n \\ x_0 = 1, \quad x_1 = 1 \end{cases}$$

① $s(z) = \sum_{n=0}^{\infty} x_n z^n$

$$s(z) = \underbrace{x_0}_{1} + \underbrace{x_1}_{1} z + \sum_{n=0}^{\infty} \underbrace{x_{n+2}}_{(x_{n+1}+x_n)} z^{n+2}$$

$$= 1 + z + z \underbrace{\sum_{n=0}^{\infty} x_{n+1} z^{n+1}}_{s(z) - x_0} + z^2 \underbrace{\sum_{n=0}^{\infty} x_n z^n}_{s(z)}$$

d'où

$$s(z) = 1 + z + z(s(z) - 1) + z^2 s(z)$$

$$s(z) = 1 + (z + z^2) s(z)$$

$$s(z) = \frac{1}{1 - z - z^2}$$

<u>Thm</u> : Si a est une suite lin. réc., alors $s_a(z)$ peut se mettre sous la forme d'une fraction rationnelle propre

② $$s(z) = \sum_{n=0}^{\infty} x_n z^n = \frac{1}{1-z-z^2} = \sum_{n=0}^{\infty} f(n)\, z^n$$

$$\Longrightarrow \boxed{x_n = f(n)}$$

Développer la fraction $\dfrac{1}{1-z-z^2}$ en serie de puissances.

a) $$\frac{1}{1-z-z^2} = \frac{\sqrt{5}}{5\,(z+\tau)} - \frac{\sqrt{5}}{5\,(z+\tau')}$$

$$\tau = \frac{1+\sqrt{5}}{2} \qquad \tau' = \frac{1-\sqrt{5}}{2}$$

Prop $$\frac{1}{(1-\rho z)^{t+1}} = \sum_{n=0}^{\infty} C_{n+t}^{t}\, \rho^n z^n .$$

Preuve : $$\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$$

D^t

$$t!\, \frac{1}{(1-z)^{t+1}} = \sum_{n=t}^{\infty} n(n-1)\cdots(n-t+1)\, z^{n-}$$

$$\frac{1}{(1-z)^{t+1}} = \sum_{n=t}^{\infty} \frac{1}{t!} \frac{n!}{(n-t)!} z^{n-t} = \sum_{n=0}^{\infty} \frac{(n+t)!}{t!\; n!} z^n$$

$\blacksquare$

$$\frac{1}{z+\tau} = \frac{1}{\tau\,(1+\frac{1}{\tau} z)} = \frac{-\tau'}{(1-\tau' z)} = -\tau' \sum_{n=0}^{\infty} \tau'^n z^n$$

$$\frac{1}{z+\tau'} = -\sum_{n=0}^{\infty} \tau^{n+1} z^n$$

$\vdots$

$$s(z) = \frac{1}{1-z-z^2} = -\frac{\sqrt{5}}{5}\sum_{n=0}^{\infty} \tau'^{\,n+1} z^n + \frac{\sqrt{5}}{5}\sum_{n=0}^{\infty} \tau^{n+1} z^n$$

$$= \sum_{n=0}^{\infty} \boxed{\frac{\sqrt{5}}{5}\left(\tau^{n+1} - \tau'^{\,n+1}\right)}\, z^n$$

forme close pour x_n

Dans les notes, autre exemple pour obtenir la suite des termes d'indice pair

$$\begin{array}{ccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1, & 1, & 2, & 3, & 5, & 8, & 13, & 21, & 34, & 55, & 89, \ldots \end{array}$$

$1, 2, 5, 13, 34, 89, \ldots$

Une application : Les nombres de Catalan

1)

$$a_0 \cdot a_1 \cdot a_2 \cdot a_3 \qquad n+1 \text{ facteurs } (n=3)$$

$$(a_0 \cdot a_1) \cdot (a_2 \cdot a_3)$$

$$a_0 \cdot (a_1 \cdot (a_2 \cdot a_3)) \qquad (a_0 \cdot (a_1 \cdot a_2)) \cdot a_3$$

$$a_0 \cdot ((a_1 \cdot a_2) \cdot a_3) \qquad ((a_0 \cdot a_1) \cdot a_2) \cdot a_3$$

ici $\mathcal{C}_3 = 5$

$$\mathcal{C}_0 = 1, \ \mathcal{C}_1 = 1, \ \mathcal{C}_2 = 2, \ \mathcal{C}_3 = 5, \ \underbrace{\mathcal{C}_n}_{\text{n-ième nbre de catalan}} = ?$$

2) les mots bien parenthésés (langage de Dyck)

aabb, ababab, ...

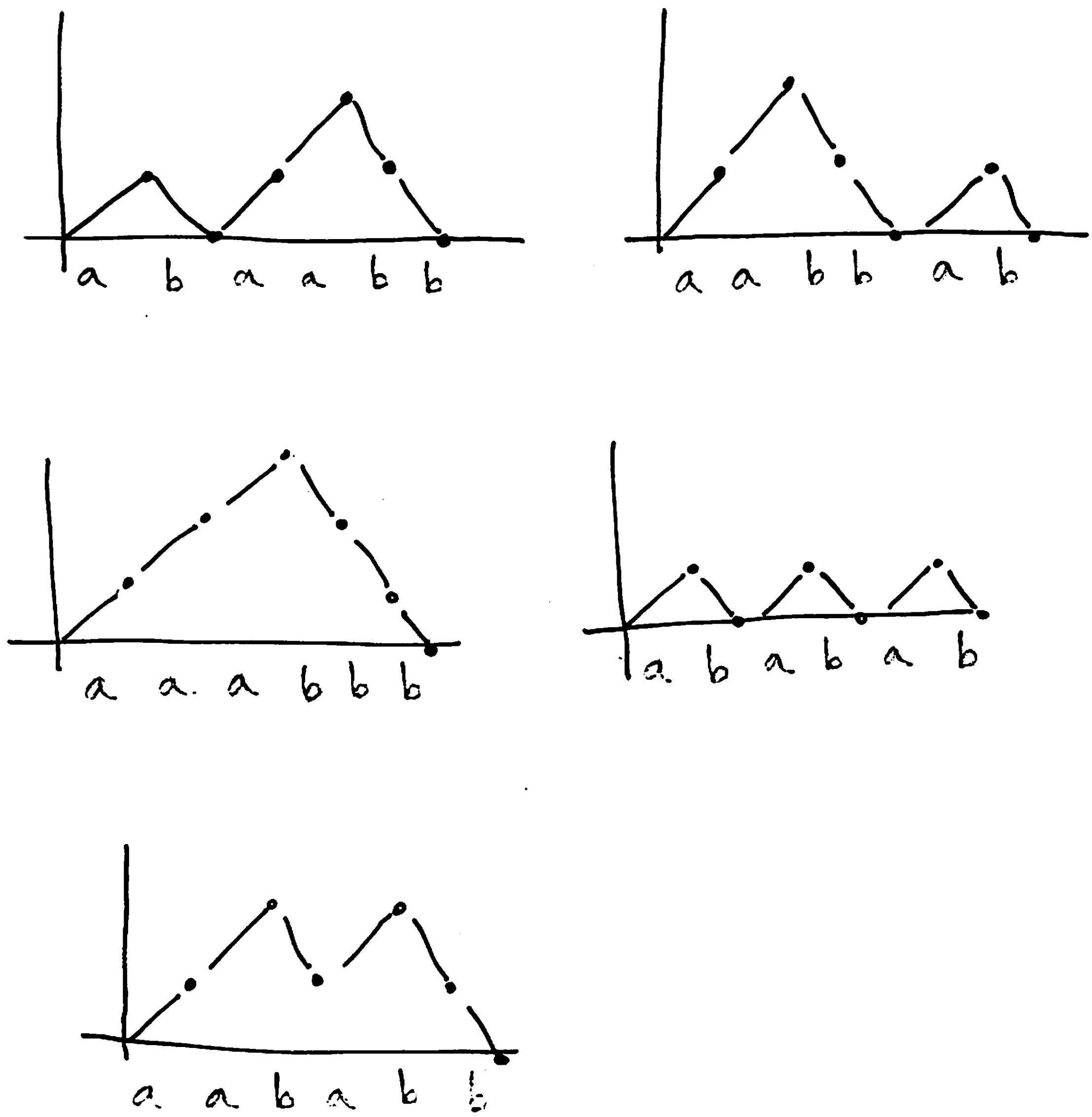
$w \in \mathcal{D}$ si $|w|_a = |w|_b$

et si pour tout préfixe v de w

$$|v|_a \geq |v|_b$$

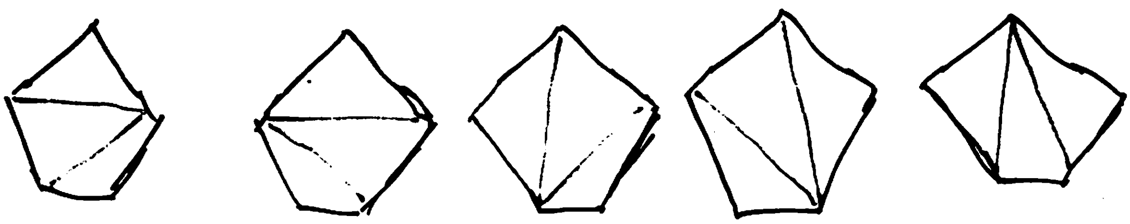
(()), ()()(), ...

a : ↗ $\qquad$ b : ↘



mots de longueur $2n = \mathcal{C}_n$.

3) Triangulation de polygones convexes



de triangulation d'un n-gone $= \mathcal{C}_{n-2}$

formule close pour $\mathcal{C}_n$ ...

$n+1$ facteurs : $a_0 \quad a_1 \quad a_2 \quad \cdots \quad a_{n-1} \quad a_n$

$$a_0 \cdot (a_1 \quad \cdots \quad a_n) \qquad \mathcal{C}_0 \cdot \mathcal{C}_{n-1}$$

$$(a_0 \quad a_1) \cdot (a_2 \quad \cdots \quad a_n) \qquad \mathcal{C}_1 \cdot \mathcal{C}_{n-2}$$

$$(a_0 \quad a_1 \quad a_2) \cdot (a_3 \quad \cdots \quad a_n) \qquad \mathcal{C}_2 \cdot \mathcal{C}_{n-3}$$

$$\vdots \qquad\qquad \vdots$$

$$(a_0 \quad \cdots \quad a_{n-1}) \cdot a_n \qquad \mathcal{C}_{n-1} \cdot \mathcal{C}_0$$

le dernier produit

$$\boxed{\mathcal{C}_n = \sum_{i=0}^{n-1} \mathcal{C}_i \, \mathcal{C}_{n-i-1}} \qquad n \geq 1$$

$$\mathcal{S}_{\mathcal{C}}(z) = \sum_{n=0}^{\infty} \mathcal{C}_n \, z^n$$

$$= \mathcal{C}_0 + \sum_{n=1}^{\infty} \mathcal{C}_n \, z^n$$

$$= 1 + \sum_{n=1}^{\infty} \left(\sum_{i=0}^{n-1} \mathcal{C}_i \, \mathcal{C}_{n-i-1} \right) z^n$$

$$s_{\mathcal{C}}(z) = 1 + \sum_{n=1}^{\infty} \Big(\sum_{i=0}^{n-1} \mathcal{C}_i \, \mathcal{C}_{n-i-1} \Big) \underbrace{z^n}_{z^i z^{n-i}}$$

$$= 1 + \underbrace{\sum_{i=0}^{\infty} \mathcal{C}_i z^i}_{s_{\mathcal{C}}(z)} \; \underbrace{\sum_{n=i+1}^{\infty} \mathcal{C}_{n-1-i} z^{n-i}}_{z \, s_{\mathcal{C}}(z)}$$

$$\boxed{z \, s_{\mathcal{C}}^2 - s_{\mathcal{C}} + 1 = 0}$$

$$\Delta = 1 - 4z$$

$$s_{\mathcal{C}} = \frac{1 \pm \sqrt{1-4z}}{2z}$$

$$s_{\mathcal{C}}(0) = \mathcal{C}_0 = 1 \quad \Rightarrow \quad s_{\mathcal{C}}(z) = \frac{1 - \sqrt{1-4z}}{2z}$$

Il ne reste plus qu'à développer en série de puissances...

<u>Proposition</u> : $t \in \mathbb{R} \setminus \mathbb{N}$, $\quad (1+z)^t = \sum_{n=0}^{\infty} C_t^n z^n$

$t \in \mathbb{R}$, $n \in \mathbb{N}$ $\quad C_t^n := \dfrac{t(t-1)\ldots(t-n+1)}{n!} = \dfrac{t^{\underline{n}}}{n!}$

<u>Preuve</u> : $|z| < 1$, Taylor

$$(1+z)^t = 1 + z \underbrace{D_z (1+z)^t \Big|_{z=0}}_{t(1+z)^{t-1}\big|_{z=0} = t} + \frac{z^2}{2!} \underbrace{D_z^2 (1+z)^t \Big|_{z=0}}_{t \cdot t-1}$$

$$+ \cdots$$

donc $\sqrt{1+z} = (1+z)^{1/2} = \sum_{n=0}^{\infty} C_{1/2}^{n}\, z^{n}$

$$\sqrt{1-4z} = \sum_{n=0}^{\infty} C_{1/2}^{n}\, (-4z)^{n}$$

$$= 1 + \sum_{n=1}^{\infty} \frac{1}{2n}\, C_{-1/2}^{n-1}\, (-4z)^{n}$$

car $C_{1/2}^{n} = \frac{1}{n!}\left(\frac{1}{2}\right)^{\underline{n}} = \frac{1}{n!}\,\frac{1}{2}\,\underbrace{\left(-\frac{1}{2}\right)\cdots\left(\frac{1}{2}-n+1\right)}_{\left(-\frac{1}{2}\right)^{\underline{n-1}}}$

$$= \frac{1}{2n}\,\underbrace{\frac{1}{(n-1)!}\left(-\frac{1}{2}\right)^{\underline{n-1}}}_{C_{-1/2}^{n-1}}$$

<u>Lemme</u> : $k \in \mathbb{N},\ r \in \mathbb{R}$

i) $C_{r}^{k} = (-1)^{k}\, C_{k-r-1}^{k}$

ii) $C_{-1/2}^{k} = \left(-\frac{1}{4}\right)^{k} C_{2k}^{k}$

$$s_{\mathcal{C}}(z) = \frac{1-\sqrt{1-4z}}{2z} = -\frac{1}{2z}\sum_{n=1}^{\infty} \frac{1}{2n}\, C_{-1/2}^{n-1}\, (-4z)^{n}$$

$$= \sum_{n=1}^{\infty} \frac{1}{n}\, C_{-1/2}^{n-1} (-4z)^{n-1}$$

$$= \sum_{n=0}^{\infty} \frac{1}{n+1}\, \boxed{C_{-1/2}^{n}}\, (-4z)^{n} = \sum_{n=0}^{\infty} \frac{C_{2n}^{n}}{n+1}\, z^{n}$$

d'où le n-ième nombre de Catalan

$$\mathcal{C}_n = \frac{1}{n+1} \mathcal{C}_{2n}^{n}$$

Lemme i) $\quad C_r^k = (-1)^k \, C_{k-r-1}^k \qquad k \in \mathbb{N},\ r \in \mathbb{R}$

$$k! \backslash \quad r^{\underline{k}} = r(r-1)(r-2)\ldots(r-k+1)$$
$$= (-1)^k (-r)(1-r)\ldots(k-1-r)$$
$$= (-1)^k (k-1-r)^{\underline{k}} \qquad / k!$$

ii) $\quad C_{-1/2}^k = \left(-\frac{1}{4}\right)^k C_{2k}^k \qquad k \in \mathbb{N}$, .

On a $\quad r^{\underline{k}} \left(r-\frac{1}{2}\right)^{\underline{k}} = \dfrac{(2r)^{\underline{2k}}}{2^{2k}} \qquad (*)$

$$r^{\underline{k}} \left(r-\tfrac{1}{2}\right)^{\underline{k}} = r\left(r-\tfrac{1}{2}\right)(r-1)\left(r-\tfrac{3}{2}\right)\ldots(r-k+1)\left(r-k+\tfrac{1}{2}\right)$$
$$= \frac{2r}{2}\,\frac{(2r-1)}{2}\,\frac{(2r-2)}{2}\ldots\frac{(2r-2k+2)}{2}\,\frac{(2r-2k+1)}{2}$$

$\dfrac{(*)}{k!^2}$:
$$\underbrace{\frac{r^{\underline{k}}}{k!}}_{C_r^k}\ \underbrace{\frac{\left(r-\frac{1}{2}\right)^{\underline{k}}}{k!}}_{C_{r-\frac{1}{2}}^k} = \underbrace{\frac{(2r)^{\underline{2k}}}{2k!}}_{C_{2r}^{2k}}\ \underbrace{\frac{2k!}{k!\,k!}}_{C_{2k}^k}\ \frac{1}{2^{2k}}$$

$k = r = n \in \mathbb{N}$:
$$\underbrace{C_{n-\frac{1}{2}}^n}_{(-1)^n C_{n-(n-\frac{1}{2})-1}^n} = \frac{1}{2^{2n}} C_{2n}^n \quad \Bigg\} \quad C_{-1/2}^n = \left(\frac{-1}{4}\right)^n C_{2n}^n$$

$$\mathscr{C}_n = \frac{1}{n+1} C_{2n}^{n}$$

$$= \frac{1}{n+1} \frac{2n!}{n!\,n!}$$

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

$$\mathscr{C}_n \sim \frac{1}{n+1}\, 2\sqrt{\pi n} \left(\frac{2n}{e}\right)^{2n} \frac{1}{2\pi n} \left(\frac{e}{n}\right)^{2n}$$

$$\sim \frac{1}{n+1} \frac{1}{\sqrt{\pi n}}\, 2^{2n}$$

Systèmes d'équations linéaires récurrentes.

FIN