Table des matières

1 Développements Algèbre

1.1 Unicité de la représentation des groupes abéliens finis

Références *: [Francinou* et al.*, a] p.64*

1.2 Théorème de Brauer

Références : *[Mansuy et Mneimné,] p.55*

Lemme :

Deux permutation $\sigma, \tau \in \mathfrak{S}_n$ sont conjugués ssi σ et τ ont autant de cycles de même longueur.

Définition :

Pour $\sigma \in \mathfrak{S}_n$, on note P_σ la matrice de permutation associée.

Lemme :

L'application $\sigma \in \mathfrak{S}_n \mapsto P_\sigma \in GL_n(\mathbb{C})$ est un morphisme de groupes.

Théorème (Brauer) :

Soient $\sigma, \tau \in \mathfrak{S}_n$, alors : σ et τ sont conjugués dans $\mathfrak{S}_n$ ssi P_σ et P_τ sont semblables dans $GL_n(\mathbb{C})$

preuve :

Supposons que $\sigma = \gamma\tau\gamma^{-1}$

Alors $P_\sigma = P_\gamma P_\tau P_{\gamma^{-1}} = P_\gamma P_\tau P_\gamma^{-1}$

Supposons que P_σ et P_τ sont semblables

Soit $c_k(\sigma)$ le nombre de cycles de longueur k dans la décomposition en cycles à supports disjoints de σ.

Montrons que $\chi_{P_\sigma} = \prod_{k=1}^{n} \left(X^k - 1\right)^{c_k(\sigma)}$

σ s'écrit $\sigma = (x_1^1 \cdots x_{l_1}^1) \cdots (x_1^r \cdots x_{l_r}^r)$ la décomposition en cycles à supports disjoints de σ

Soit $(e_1, \cdots, e_n)$ la base canonique. En passant de la base canonique à a base $(e_{x_1^1}, \cdots e_{x_{l_1}^1}, \cdots, e_{x_1^r}, \cdots e_{x_{l_r}^r})$, on sait que P_σ est semblable à :

$$\begin{pmatrix} C_{l_1} & & \\ & \ddots & \\ & & C_{l_r} \end{pmatrix}$$

où $\forall 1 \leq j \leq r, C_{l_j} = \left.\begin{pmatrix} 0 & \cdots & 0 & 1 \\ 1 & \ddots & & 0 \\ & \ddots & 0 & \vdots \\ & & 1 & 0 \end{pmatrix}\right\} l_j$

On a donc : $\chi_{P_\sigma} = \prod_{j=1}^{r} \begin{vmatrix} \mathrm{X} & \cdots & 0 & -1 \\ -1 & \ddots & & 0 \\ & \ddots & \mathrm{X} & \vdots \\ & & -1 & \mathrm{X} \end{vmatrix} = \prod_{j=1}^{r} X^j - 1$ (faire une décompostion selon la première ligne)

Montrons que $\forall 1 \leq k \leq n, \sum_{k|l} c_l(\sigma) = \sum_{k|l} c_l(\tau)$ $(*)$

Soit $1 \leq k \leq n$, $e^{2i\pi/k}$ est racine de $X^l - 1$ ssi $k|l$. De plus, $X^l - 1$ est à racines simples (car $\mathbb{C}$ est de caractéristique nulle).

Donc l'ordre de $e^{2i\pi/k}$ comme racine de χ_{P_σ} est $\sum_{k|l} c_l(\sigma)$

Et, comme P_σ et P_τ sont semblables, on a : $\chi_{P_\sigma} = \chi_{P_\tau}$

D'où $\forall 1 \leq k \leq n, \sum_{k|l} c_l(\sigma) = \sum_{k|l} c_l(\tau)$

Montrons que $\forall 1 \leq k \leq n, c_k(\sigma) = c_k(\tau)$

On fait un raisonnement par récurrence descendante sur k.

En prenant $k = n$ dans la formule $(*)$ on a : $c_n(\sigma) = c_n(\tau)$

Soit $1 \leq k < n$, supposons que $\forall d > k, c_d(\sigma) = c_d(\tau)$. Montrons que $c_k(\sigma) = c_k(\tau)$.

La formule $(*)$ donne : $\sum_{k|l} c_l(\sigma) = \sum_{k|l} c_l(\tau)$

Par ailleurs, on a : $\sum_{k|l} c_l(\sigma) = c_k(\sigma) + \sum_{k|l, k<l} c_l(\sigma) = c_k(\sigma) + \sum_{k|l, k<l} c_l(\tau) = c_k(\sigma) - c_k(\tau) + \sum_{k|l} c_l(\tau)$

D'où $c_k(\sigma) = c_k(\tau)$

■

1.3 Les automorphismes de $\mathfrak{S}_n$

Références *: [Francinou* et al.*, a] p.74, [Perrin,] p.31*

1.4 Théorème de Burnside

Références : *[Francinou* et al., *b] p.185*

Lemme :

Soit $A \in \mathcal{M}_n(\mathbb{C})$. Si $\forall k \geq 1, tr\left(A^k\right) = 0$, alors A est nilpotente.

preuve :

Soient $\lambda_1, \cdots, \lambda_r$ les valeurs propres non nulles de A, notons $m_1, \cdots, m_r$ leur multiplicités respectives (donc $\forall i, m_i \geq 1$).

On a : $\forall k \geq 1, tr(A^k) = \sum_{j=1}^{r} m_j \lambda_j^k = 0$ (par hypothèse).

Pour $1 \leq k \leq r$, on obtient le système suivant :

$$\begin{pmatrix} \lambda_1 & \lambda_2 & \cdots & \lambda_r \\ \lambda_1^2 & \lambda_2^2 & \cdots & \lambda_r^2 \\ \vdots & \vdots & & \vdots \\ \lambda_1^r & \lambda_2^r & \cdots & \lambda_r^r \end{pmatrix} \begin{pmatrix} \mathrm{m}_1 \\ \mathrm{m}_2 \\ \vdots \\ \mathrm{m}_r \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

La matrice à gauche est inversible (en effet, son déterminant vaut $\lambda_1 \cdots \lambda_r \prod_{i<j} (\lambda_j - \lambda_i) \neq 0$)

D'où $\forall 1 \leq i \leq r, m_i = 0$

Ceci n'est possible que si $r = 0$.

Donc 0 est l'unique valeur propre de A.

Donc A est nilpotente (car $\mathbb{C}$ est algébriquement clos). ■

Théorème (Burnside) :

Soit G sous-groupe de $GL_n(\mathbb{C})$ d'exposant fini (ie $\exists d \in \mathbb{N}, \forall A \in G, A^d = I_n$). Alors G est fini.

preuve :

Montrons qu'il existe une base $(M_1, \cdots, M_r)$ de $Vect(G)$ tel que $\forall i, M_i \in G$

Construisons une famille libre récursivement.

Soit $M_1 \in G$ quelconque.

Supposons que l'on a une famille libre de G : $(M_1, \cdots, M_k)$

Si $(M_1, \cdots, M_k)$ est une base de $Vect(G)$, alors il n'y a rien à faire.

Sinon, Soit $A \in Vect(G) \backslash Vect(M_1, \cdots, M_k)$. On peut donc écrire $A = \sum_{i=1}^{s} \lambda_i A_i$ où $A_1, \cdots, A_s \in G$.

On sait alors que $\exists 1 \leq i_0 \leq r, A_{i_0} \notin Vect(M_1, \cdots, M_k)$ (sinon A appartiendrait aussi à $Vect(M_1, \cdots, M_k)$, ce qui est faux).

On pose alors $M_{k+1} = A_{i_0} \in G \backslash Vect(M_1, \cdots, M_k)$. Comme $(M_1, \cdots, M_k)$ est libre, il en est de même de $(M_1, \cdots, M_{k+1})$.

Le processus précédent s'arrête en au plus n étapes, et permet de construire une base $(M_1, \cdots M_r)$ de $Vect(G)$ telle que $\forall 1 \leq i \leq r, M_i \in G$.

On définit la fonction suivante :

$$f : A \in G \mapsto (tr(AM_i))_{1 \leq i \leq r} \in \mathbb{C}^r$$

Montrons que f est injective

Soient $A, B \in G$ tel que $f(A) = f(B)$. Montrons que $A = B$.

Par linéarité de la trace et de la multiplication matricielle, on a : $\forall M \in G, tr(AM) = tr(BM)$

Soit $D = AB^{-1} \in G$. Montrons que $D = I_n$ en montrant que $D - I_n$ est nilpotente et diagonalisable.

Alors $\forall k \in \mathbb{N}, tr\left(D^{k+1}\right) = tr\left(AB^{-1}D^k\right) = tr\left(BB^{-1}D^k\right) = tr\left(D^k\right)$

Donc $\forall k \in \mathbb{N}, tr\left(D^k\right) = tr(I_n) = n$

Donc $\forall k \geq 1, tr\left((D - I_n)^k\right) = tr\left(\sum_{j=0}^{k} \binom{j}{k}(-1)^j D^{k-j}\right) = \sum_{j=0}^{k} \binom{j}{k}(-1)^j tr\left(D^{k-j}\right) = (1-1)^k = 0$

Donc $D - I_n$ est nilpotente (d'après le lemme)

De plus D est diagonalisable, car D est annulée par le polynôme $X^d - I_n$ qui est scindé à racines simples sur $\mathbb{C}$.

Donc $D - I_n$ est aussi diagonaliable (en effet, toute matrice diagonalisable est co-diagonalisable avec I_n)

D'où $D - I_n = 0$

ie $A = B$

Donc f est bien injective.

Montrons que G est fini

Il suffit de montrer que $f(G)$ est fini (puisque f est injective).

$f(G) \subseteq \prod_{i=1}^{r} \{tr(AM_i) : A \in G\} \subseteq \{tr(A) : a \in G\}^r$ puisque $\forall A \in G, \forall 1 \leq i \leq r, AM_i \in G$

De plus, $\forall A \in G, tr(A) \in \left\{\sum_{j=1}^{n} \lambda_j : \lambda_1, \cdots, \lambda_n \in \mathbb{U}_d\right\}$ puisque $X^d - 1$ annule toute matrice $A \in G$.

D'où $f(G) \subseteq \left\{\sum_{j=1}^{n} \lambda_j : \lambda_1, \cdots, \lambda_n \in \mathbb{U}_d\right\}^r$ qui est fini.

■

1.5 Structure de $\mathcal{U}(\mathbb{Z}/n\mathbb{Z})$

Références *: [Perrin,] p.25*

1.6 Critère d'Eisenstein

Références : *[Francinou* et al., *a] p.188*

Lemme :

Soit A un anneau intègre, alors $A[X]$ est intègre.

Lemme :

Soit A un anneau. Soient $n \in \mathbb{N}^*, a \in A\backslash\{0\}, P, Q \in A[X]$ tels que $aX^n = B.C$. Alors B et C sont des monômes.

preuve :

Écrivons $B = \sum_{i=0}^{k} b_i X^i$ et $C = \sum_{j=0}^{l} c_j X^j$ avec $n = k + l$.

Soient $i_0 = \min\{0 \leq i \leq k \ : \ b_i \neq 0\}$ et $j_0 = \min\{0 \leq j \leq l \ : \ c_j \neq 0\}$. Il suffit alors de montrer que $i_0 = k$ et $j_0 = l$.

Mais, si ce n'était pas le cas, on aurait :

$$aX^n = b_k.c_l X^n + b_{i_0} c_{j_0} X^{i_0+j_0} + \sum_{u=i_0+j_0+1}^{n-1} d_u X^u$$

Ce qui n'est possible que si $b_{i_0} c_{j_0} = 0$, ie $b_{i_0} = 0$ ou $c_{j_0} = 0$, ce qui est absurde. ■

Définition :

Soit $A = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$. On note $c(A)$ le pgcd des $(a_k \ : \ 0 \leq k \leq n)$. $c(A)$ est le contenu de A.
On dit que Z est primitf si $c(A) = 1$

Lemme :

Pour $A, B \in \mathbb{Z}[X], c(A.B) = c(A)c(B)$

preuve :

Montrons d'abord le résultat dans le cas où $c(A) = c(B) = 1$

On écrit $A = \sum_{k=0}^{n} a_k X^k$ et $B = \sum_{k=0}^{m} b_k X^k$.

Soit $C = A.B = \sum_{k=0}^{m+n} c_k X^k$. Montrons par l'absurde que $c(C) = 1$.

Soit donc p un diviseur premier de $c(C)$. On sait donc que dans $\mathbb{Z}/p\mathbb{Z}[X]$, $\overline{C} = \overline{A}.\overline{B} = 0$. Comme $\mathbb{Z}/p\mathbb{Z}$ est un corps, on sait par le lemme ci-dessus, que $\mathbb{Z}/p\mathbb{Z}[X]$ est intègre. On déduit que $\overline{A} = 0$ ou $\overline{B} = 0$. Ce qui signifie exactement que p divise $c(A)$ ou p divise $c(B)$. Ce qui est absurde puisque, $c5a) = c(B) = 1$ par hypothèse.

D'où : $c(A) = c(B) = 1 \Rightarrow c(A.B) = 1$

Montrons le cas général.

Il est clair que $\frac{A}{c(A)}$ et $\frac{B}{c(B)}$ sont primitifs (par dérinition du contenu et de la primitivité), de plus, il est évident que $\forall k \in \mathbb{N}^*, \forall C \in \mathbb{Z}[X], c(k.C) = k.c(C)$.

Donc en écrivant $A.B = c(A).c(B)\frac{A}{c(A)}\frac{B}{c(B)}$, et en utilisant ce qui a déjà été démontré, on obtient : $c(A.B) = c(A).c(B)$

■

Lemme :

Soit $A \in \mathbb{Z}[X]$. Si A n'est pas irréductible dans $\mathbb{Q}[X]$, alors $\exists B, C \in \mathbb{Z}[X]$ tels que $A = B.C$ et $\deg B, \deg C \geq 1$

preuve :

Si A n'est pas irréductible dans $\mathbb{Q}[X]$, alors on peut écrire $A = B.C$ où $B, C \in X]$ et $\deg B, \deg Q \geq 1$.

Soient $\beta, \gamma \in \mathbb{N}^*$ tels que $\beta B, \gamma C \in \mathbb{Z}[X]$ (par exemple β est le produit des dénominateurs des coefficients de B).

On a donc : $\beta.\gamma A = \beta B.\gamma C$

D'où : $\beta.\gamma c(A) = c(\beta B)c(\gamma C)$

Donc on peut écrire A sous la forme :

$$A = B.C = \beta.\gamma.c(A)\frac{B}{c(\beta B)}\frac{C}{c(\gamma C)}$$

Et $\frac{B}{c(\beta B)}, \frac{C}{c(\gamma C)}$ sont des polynômes de $\mathbb{Z}[X]$ de degré supérieur à 1.

■

Théorème (Critère d'Eisenstein) :

Soient $A = \sum_{k=0}^{n} a_k X^k \in \mathbb{Z}[X]$ et p un nombre premier. On suppose que :

- p ne divise pas a_n
- pour $0 \leq k \leq n-1$, p divise a_k
- p^2 ne divise pas a_0

Alors : A est irréductible dans $\mathbb{Q}[X]$

preuve :

Supposons que A n'est pas irréductible dans $\mathbb{Q}[X]$. Alors, par le lemme précédent, $\exists B, C \in \mathbb{Z}[X], A = B.C$ et $\deg B, \deg C > 1$.

Écrivons $B = \sum_{i=0}^{k} b_i X^i$ et $C = \sum_{j=0}^{l} c_j X^j$ où $k = \deg B$ et $l = \deg C$.

En projetant $A = B.C$ dans $\mathbb{Z}/p\mathbb{Z}[X]$, on a :

$$\overline{a_n} X^n = \overline{BC}$$

On sait alors que $\overline{B}$ et $\overline{C}$ sont des monômes. On écrit donc $B = \overline{b_i} X^i$ et $B = \overline{c_j} X^j$ où $i \leq k$ et $j \leq l$.

En passant au degré dans l'égalité $\overline{a_n} X^n = \overline{BC}$, on a : $n = i + j \leq k + l = n$. Donc les inégalités $i \leq k$ et $j \leq l$ sont en faites des égalités. On sait alors que $\overline{B} = \overline{b_k} X^k$ et $\overline{C} = \overline{c_l} X^l$, et comme $k = \deg B \geq 1$ et $l = \deg C \geq 1$, on sait que $\overline{b_0} = 0 = \overline{c_0}$. Autrement dit, p divise b_0 et p divise c_0, donc p^2 divise $b_0 c_0 = a_0$, ce qui est exclu par la troisième hypothèse. ■

1.7 Théorème des deux carrés

Lemme :

Soit K un corps fini commutatif de caractéristique différente de 2, de cardinal q, et soit a un élément de K. Alors a est un carré dans K ssi $a^{\frac{q-1}{2}} = 1$

preuve :

Montrons que $\prod_{x \in K^*} x = -1$

On considère la relation d'équivalence R sur K^* : $xRy \Leftrightarrow y = x$ ou $y = x^{-1}$

La classe d'équivalence d'un $x \in K^*$ est $\{x, x^{-1}\}$

1 et -1 sont les seuls éléments dont les classes d'équivalences n'ont qu'un seul élément. En effet, $|\{x, x^{-1}\}| = 1 \Rightarrow x = x^{-1} \Rightarrow x$ racine de $X^2 - 1$. Comme c'est un polynôme de degré 2, il a au plus deux racines, et 1 et -1 sont bien des racines de $X^2 - 1$.

Finalement, si on note $x_1, \cdots x_r$ des représentants des classes d'équivalences, on peut calculer $\prod_{x \in K^*} x$ en regroupant les termes par classes d'équivalences :

$$\prod_{x \in K^*} x = 1.(-1).\prod_{i=1}^{r} x_i.x_i^{-1} = -1$$

Montrons que (a est un carré $\Rightarrow a^{\frac{q-1}{2}} = 1$) et ($a$ n'est pas un carré $\Rightarrow a^{\frac{q-1}{2}} = -1$)

Si a est un carré, alors on écrit $a = x^2$. Donc $a^{\frac{q-1}{2}} = x^{q-1} = 1$ (par le théorème de Lagrange).

Si a n'est pas un carré, on considère la relation d'équivalence S sur K^* : $xSy \Leftrightarrow y = x$ ou $y = ax^{-1}$

La classe d'équivalence d'un $x \in K^*$ est $\{x, ax^{-1}\}$. Chaque classe est de cardinal 2. En effet, si $|\{x, ax^{-1}\}| = 1$, alors $x = ax^{-1}$ ie $a = x^2$ ce qui est faux par hypothèse.

En calculant $\prod_{x \in K^*} x$ en regroupant les termes par classes d'équivalences, on a :

$$-1 = \prod_{x \in K^*} x = \prod_{i=1}^{r} x_i.a.x_i^{-1} = a^r = a^{\frac{q-1}{2}}$$

■

Théorème :

Soit p premier. Alors $\exists x, y \in \mathbb{N}, p = x^2 + y^2$ ssi $p = 2$ ou $p \equiv 1 \pmod 4$

preuve :

Supposons que $p = x^2 + y^2$ **avec** $x, y \in \mathbb{N}$

on sait que $x^2 \equiv 0$ ou $1 \pmod 4$

donc $p = x^2 + y^2 \equiv 0$ ou 1 ou 2 $\pmod 4$

de plus, il est impossible que $p \equiv 0 \pmod 4$ (car p est premier)

et $p \equiv 2 \pmod 4$ signifie exactement que $p = 2$ (puisque c'est le seul nombre premier pair).

Réciproquement, supposons que $p \equiv 1 \pmod 4$

Rq : On peut se passer du cas trivial $p = 2 = 1^2 + 1^2$.

on sait alors que $(-1)^{\frac{p-1}{2}} = 1$, donc -1 est un carré dans $\mathbb{F}_p$ (d'après le Lemme).

Soit a dans $\mathbb{F}_p$ tel que $\overline{-1} = a^2$

Soit $\psi : (x, y) \in \left[\!\left[0, \left\lfloor \sqrt{p} \right\rfloor\right]\!\right]^2 \longmapsto \overline{x} - a.\overline{y} \in \mathbb{F}_p$

On a $\left|\left[\!\left[0, \left\lfloor \sqrt{p} \right\rfloor\right]\!\right]^2\right| = \left(\left\lfloor \sqrt{p} \right\rfloor + 1\right)^2 > \sqrt{p}^2 = p = |\mathbb{F}_p|$

Donc ψ ne peut pas être injective. Soient donc $(x_1, y_1), (x_2, y_2) \in \left[\!\left[0, \left\lfloor \sqrt{p} \right\rfloor - 1\right]\!\right]^2$ tels que $(x_1, y_1) \neq (x_2, y_2)$ et $\overline{x_1} - a.\overline{y_1} = \overline{x_2} - a.\overline{y_2}$

On a donc $\overline{x_1 - x_2} = a.\overline{y_1 - y_2}$

donc $\overline{x_1 - x_2}^2 = -\overline{y_1 - y_2}^2$

d'où $\overline{(x_1 - x_2)^2 + (y_1 - y_2)^2} = 0$

On a donc que $(x_1 - x_2)^2 + (y_1 - y_2)^2$ est un multiple de p.

Et on a aussi que $(x_1 - x_2)^2 + (y_1 - y_2)^2 > 0$ (puisque $(x_1, y_1) \neq (x_2, y_2)$)

Et $(x_1 - x_2)^2 + (y_1 - y_2)^2 < 2p$

Comme p est le seul multiple de p dans $]0, 2p[$, on a nécessairement $p = (x_1 - x_2)^2 + (y_1 - y_2)^2$

■

1.8 Classification des formes quadratiques non dégénérées sur les corps finis de caractéristique différente de 2

Références *: [Francinou* et al.*, c] p.217*

1.9 Nombres de polynômes unitaires, de degré n, irréductible sur $\mathbb{F}_q$

Soit q une puissance d'un nombre premier.

Soit K_n l'ensemble des polynômes de $\mathbb{F}_q[X]$ unitaires, irréductibles et degré n.

Soit $I_n = |K_n|$.

Dans un premier temps, montrons que $q^n = \sum_{d|n} d.I_d$

Pour cela, il suffit de montrer que $X^{q^n} - X = \prod_{d|n} \prod_{P \in K_d} P$.

Soit $Q = X^{q^n} - X$.

Montrons qu'il n'y a pas de facteurs carré dans la décomposition en produits de polynômes irréductibles sur $\mathbb{F}_q$ de Q.

Par l'absurde, supposons qu'il existe $P \in \mathbb{F}_q[X]$ irréductible sur $\mathbb{F}_q$ tel que $P^2|Q = X^{q^n} - X$. On aurait alors $P|Q' = -1$ ce qui est absurde.

Il suffit alors de montrer que les polynômes qui apparaissent dans la décomposition en facteurs premiers sur $\mathbb{F}_q$ de Q sont exactement les polynômes de $\bigcup_{d|n} K_d$.

Soit $P \in \mathbb{F}_q[X]$ irréductible et unitaire tel que $P|Q$, notons d son degré. Montrons que $d|n$

Soit $a \in \mathbb{F}_{q^n}$ une racine de P. Par multiplicativité des degrés, on a : $[\mathbb{F}_{q^n} : \mathbb{F}_q] = [\mathbb{F}_{q^n} : \mathbb{F}_q[a]] . [\mathbb{F}_q[a] : \mathbb{F}_q]$

d'où : $n = [\mathbb{F}_{q^n} : \mathbb{F}_q[a]] .d$

Soit $d|n$, et soit $P \in K_d$. Montrons que $P|Q$.

Soit L le corps de décomposition de P sur $\mathbb{F}_q$.

Soit $a \in L$ une racine de P. On a donc :$[\mathbb{F}_q[a] : \mathbb{F}_q] = \deg P = d$ (car P est irréductible sur $\mathbb{F}_q$).

D'où $\mathbb{F}_q[a] \approx \mathbb{F}_{q^d} \subseteq \mathbb{F}_{q^n}$ (car $d|n$).

Donc $a^{q^n} = a$, ie a est une racine de Q.

On vient de montrer que toute racine de P est racine de Q. De plus, Q n'a que des racines simples (on a déjà montré que Q n'a pas de facteurs irréductibles au carré), donc P aussi.

On sait alors que P divise Q dans L.

Comme L est une extention de $\mathbb{F}_q$, on sait alors que P divise Q dans $\mathbb{F}_q$. (cf unicité de la division euclidienne)

Finalement, on a montré que $X^{q^n} - X = \prod_{d|n} \prod_{P \in K_d} P$

En passant au degré, on a : $q^n = \sum_{d|n} d.I_d$

Montrons que $I_n \sim \frac{q^n}{n}$

On a : $q^n \geq n.I_n$

D'où $n.I_n = q^n - \sum_{d|n, d \neq n} d.I_d \geq q^n - \sum_{d|n, d \neq n} q^d \geq q^n - \sum_{d=1}^{\lfloor n/2 \rfloor} q^d = q^n - q\frac{q^{\lfloor n/2 \rfloor}-1}{q-1} \geq q^n - q^{\lfloor n/2 \rfloor + 1} \sim q^n$

D'où $n.I_n \sim q^n$

1.10 Dimension de l'espace des formes p–linéaires alternées sur un espace de dimension n

Références *: [Francinou* et al., *b] p.5*

1.11 Décomposition effective de Dunford

Lemme :

$\forall P \in \mathbb{C}[X], \exists \widetilde{P} \in \mathbb{C}[X,Y], P(X-Y) = P(X) - YP'(X) + Y^2\widetilde{P}(X,Y)$

preuve :

Soit $P = \sum_{k=0}^{n} a_k X^k$.

Alors $P(X-Y) = \sum_{k=0}^{n} a_k \sum_{j=0}^{k} \binom{k}{j} X^{k-j}(-Y)^j = \sum_{k=0}^{n} a_k \binom{k}{0} X^{k-0} + \sum_{k=1}^{n} a_k \binom{k}{1} X^{k-1}.(-Y) + \sum_{k=2}^{n} a_k \sum_{j=2}^{k} \binom{k}{j} X^{k-j}(-Y)^j$

Donc $P(X-Y) = P(X) - YP'(X) + Y^2\widetilde{P}(X,Y)$ où $\widetilde{P}(X,Y) = \sum_{k=2}^{n} a_k \sum_{j=2}^{k} \binom{k}{j} X^{k-j}(-Y)^{j-2}$

■

Théorème :

Soit $A \in \mathcal{M}_n(K)$ trigonalisable. Soit $\chi_A = \prod_{j=1}^{d} (X-\lambda_j)^{\alpha_j}$ le polynôme caractéristique de A.

Soit $P = \prod_{j=1}^{d} (X-\lambda_j)$.

Alors :

- (i) $P = \frac{\chi_A}{\chi_A \wedge \chi_A'}$
- (ii) on peut définir la suite $\begin{cases} A_0 = A \\ A_{k+1} = A_k - P(A_k)P'(A_k)^{-1} \end{cases}$. De plus cette suite est stationnaire, et converge vers une matrice diagonale D tel que $A-D$ est nilpotente. De plus, D et $A-D$ sont des polynômes en A.

preuve :

(i)

χ_A' s'écrit $\chi_A' = \sum_{j_0=1}^{d} \alpha_{j_0}(X-\lambda_{j_0})^{\alpha_{j_0}-1} \prod_{j \neq j_0} (X-\lambda_j)^{\alpha_j}$

Soit $Q = \chi_A \wedge \chi_A'$. Comme Q divise chi_A, on sait que Q s'écrit : $Q = \prod_{j=1}^{d} (X-\lambda_j)^{\beta_j}$ où $\forall j, 0 \leq \beta_j \leq \alpha_j$

D'autre part, pour j_0 fixé, $(X-\lambda_{j_0})^{\alpha_{j_0}} - 1$ divise χ_A' (puisqu'il divise tous les termes de la somme). Et $(X-\lambda_{j_0})^{\alpha_{j_0}}$ ne divise pas χ_A'. En effet, si c'était le cas, $(X-\lambda_{j_0})^{\alpha_{j_0}}$ devrait diviser $\alpha_{j_0}(X-\lambda_{j_0})^{\alpha_{j_0}-1} \prod_{j \neq j_0} (X-\lambda_j)^{\alpha_j}$, et donc, on aurait que $(X-\lambda_{j_0})^{\alpha_{j_0}}$ divise $(X-\lambda_{j_0})^{\alpha_{j_0}-1}$. Ce qui est absurde.

Donc finalement, on a bien $Q = \prod_{j=1}^{d} (X-\lambda_j)^{\alpha_j - 1}$

(ii)

On va montrer par récurrence sur k $\begin{cases} (1)\ A_k \in K[A] \\ (2)\ P(A_k) \in P(A)^{2^k} K[A] \\ (3)\ P'(A_k) \text{ inversible et } P'(A_k)^{-1} \in K[A] \end{cases}$

initialisation : (1) et (2) sont trivialement vraies. Montrons (3).

P est scindé à racines simples, donc P et P' sont premiers entre eux. Donc P^n et P' sont premiers entre eux. Soient donc $U, V \in K[X]$ tel que $U.P^n + V.P' = 1$. Comme χ_A divise P^n, on a $P^n(A) = 0$. D'où $V(A).P'(A) = 1$, ie $P'(A)$ est inversible, et $P'(A)^{-1} = V(A)$.

hérédité :

(1) $A_{k+1} = A_k - P(A_k)P'(A_k)^{-1} \in K[A]$ car $P'(A_k)^{-1} \in K[A]$ par hypothèse de récurrence.

(2) $P(A_{k+1}) = P(A_k - P(A_k)P'(A_k)^{-1})$

En appliquant le Lemme, on obtient : $P(A_{k+1}) = P(A_k) - P(A_k)P'(A_k)^{-1}P'(A_k) - \left(P(A_k)P'(A_k)^{-1}\right)^2 R(A_k)$ où $R \in K[X]$.

D'où $P(A_{k+1}) = P(A_k)^2 P'(A_k)^{-2} R(A_k) \in P(A)^{2^{k+1}} K[A]$ puisque par hypothèse de récurrence, on a $P(A_k) \in P(A)^{2^k} K[A]$ et $A_k \in K[A]$.

(3) On ré-utilise la relation de Bézout précédente : $U.P^n + V.P' = 1$.

Comme $P(A_{k+1}) \in P(A)^{2^{k+1}} K[A]$ et que $P(A)^n = 0$, on sait que $P(A_{k+1})^n = 0$. D'où $P'(A_{k+1})V(A_{k+1}) = 1$, ie $P'(A_{k+1})$ est inversible et $P'(A_{k+1})^{-1} = V(A_{k+1}) \in K[A_{k+1}] \subseteq K[A]$, puisque $A_{k+1} \in K[A]$ (on l'a déjà montré).

On a donc montré que $\forall k$, $\begin{cases} \text{(1) } A_k \in K[A] \\ \text{(2) P}(A_k) \in P(A)^{2^k} K[A] \\ \text{(3) P'}(A_k) \text{ inversible et } P'(A_k)^{-1} \in K[A] \end{cases}$

La suite $(A_k)_k$ est constante à partir du rang $k_0 = \lceil \log_2 n \rceil$ (d'après (2)).

Soit $D = A_{k_0}$. D est diagonalisable puisque $P(D) = 0$ (cf (2)) et P scindé à racines simples.

Et $A - D = \sum_{k=0}^{k_0-1} A_k - A_{k+1}$. Comme les matrices $A_k - A_{k+1} = P(A_k)P'(A_k)^{-1}$ sont nilpotentes et commutent deux-à-deux (ce sont toutes des polynômes en A), on sait que $A - D$ est nilpotente.

Ainsi, $A = D + (A - D)$ avec D diagonalisable, $A - D$ nilpotentes, et D et $A - D$ sont des polynômes en A. On a donc bien trouvé la décomposition de Dunford de A.

■

1.12 Etude du dual de $M_n(K)$

Références *: [Francinou* et al.*, a] p.329-331*

1.13 Ellipsoïde de John-Loewner

Références *: [Francinou* et al.*, c] p.229*

2 Développements Analyse

2.1 Equivalence des normes sur les $\mathbb{R}$–espaces vectoriels de dimension finie

Références *: [Choquet,] p.8*

Proposition :

Dans $\mathbb{R}$ tout segment est compact.

preuve :

Soient $a < b$, soit $[a,b] \subseteq \bigcup_{i\in I} O_i$ un recouvrement ouvert de $[a,b]$.

Soit $X = \left\{ a \leq x \leq b : \exists J \subseteq I, J \text{ est fini et } [a,x] \subseteq \bigcup_{j\in J} O_j \right\}$

$X \neq \varnothing$ (car $a \in X$) et X est majoré par b, soit donc $c = \sup X$.

On sait que $c > a$ (puisqu'il existe i tel que $a \in O_i$, et donc il existe $a < x < b$ tel que $[a,x] \subseteq O_i$)

Montrons que $c \in X$

Soit i_0 tel que $x \in O_{i_0}$. soit $c' < c$ tel que $[c',c] \subseteq O_{i0}$. Soit $c'' \in [c',c]$ tel que $c'' \in X$ (d'après les propriétés de la borne supérieure). Soit donc $J \subseteq I$ fini tel que $[a,c''] \subseteq \bigcup_{j\in J} O_j$.

On a alors : $[a,c] = [a,c''] \cup [c'',c] \subseteq \bigcup_{j\in J\cup\{i_0\}} O_j$

donc $c \in X$.

Montrons que $c = b$

Supposons que $c < b$. Reprenons les notations précédentes, soit $c < d < b$ tel que $[c,d] \subseteq O_{i_0}$.

On a alors : $[a,d] = [a,c] \cup [c,d] \subseteq \bigcup_{j\in J\cup\{i_0\}} O_j$

donc $d \in X$ et $d > c = \sup X$. C'est absurde.

D'où $c = b$.

Finalement $b = c \in X$. Donc on peut extraire un sous-recouvrement fini de $[a,b]$.

■

Proposition :

Dans $(\mathbb{R}^n, \|.\|_\infty)$, les compacts sont les fermés bornés

preuve :

Soit A fermée et bornée dans $(\mathbb{R}^n, \|.\|_\infty)$. Alors il existe des segments $[a_i,b_i]$ tels que $A \subseteq \prod_{i=1}^{n} [a_i,b_i]$.

De plus, $\prod_{i=1}^{n} [a_i,b_i]$ est un compact pour la topologie produit (cf théorème de Tychonoff), donc est un compact pour la topologie de $(\mathbb{R}^n, \|.\|_\infty)$.

Donc A est fermé dans $(\mathbb{R}^n, \|.\|_\infty)$ et est inclus dans un compact de $(\mathbb{R}^n, \|.\|_\infty)$. Donc A est compact.

■

Théorème :

Sur $\mathbb{R}^n$ toutes les normes sur équivalentes.

preuve :

Soit N une norme quelconque sur $\mathbb{R}^n$, soit $(e_i)_{1\leq i\leq n}$ la base canonique de $\mathbb{R}^n$.
D'abord, $\forall x, N(x) = N\left(\sum_{i=1}^{n} x_i e_i\right) \leq \left(\sum_{i=1}^{n} e_i\right)\|x\|_\infty$
En particulier, N est continue dans la topologie de $(\mathbb{R}^n, \|.\|_\infty)$
Soit $C = \{x : \|x\|_\infty = 1\}$ compact pour $(\mathbb{R}^n, \|.\|_\infty)$ (car fermé et borné pour $\|.\|_\infty$)
Soit $x_0 \in C$ tel que $N(x_0) = \min_{x\in C} N(x)$.
D'où $\forall x \in \mathbb{R}^n\backslash\{0\}, N\left(\frac{x}{\|x\|_\infty}\right) \geq N(x_0)$
Donc : $\forall x \in \mathbb{R}^n, N(x) \geq N(x_0).\|x\|_\infty$

■

Conséquences :

- toute application linéaire dont l'espace de départ est un $\mathbb{R}-$espace vectoriel normé de dimension finie est continue
- le théorème de Riesz

2.2 Théorème d'Ascoli

Lemme :

Soit A une partie d'un espace métrique E, alors :

A relativement compact dans E ssi toute suite à valeurs dans A admet une sous-suite qui converge dans E.

Définition :

Soit $\mathcal{A} \subseteq \mathcal{C}(E,F)$ où E, F sont des espaces métriques.

$\mathcal{A}$ est équicontinue en $x \in E$ si : $\forall \epsilon > 0, \exists \eta > 0, \forall y \in E, d(x,y) < \eta \Rightarrow \forall f \in \mathcal{A}, d(f(x), f(y)) < \epsilon$

$\mathcal{A}$ est uniformément équicontinue sur E si : $\forall \epsilon > 0, \exists \eta > 0, \forall x, y \in E, d(x,y) < \eta \Rightarrow \forall f \in \mathcal{A}, d(f(x), f(y)) < \epsilon$

Lemme :

Soit $\mathcal{A} \subseteq \mathcal{C}(K,F)$ où K espace métrique compact, et F espace métrique (quelconque), alors :

$\mathcal{A}$ est équicontinue sur K (ie en tout point de K) ssi $\mathcal{A}$ est uniformément équicontinue sur K

Lemme :

Soit E et F des espaces métriques, tel que F est complet, soit D une partie dense dans E, et soit $f : D \longrightarrow F$ uniformément continue sur D. Alors il existe un unique prolongement continue de f sur E. De plus, ce prolongement est uniformément continue.

Théorème :

Soit $\mathcal{A} \subseteq \mathcal{C}(K,F)$ où K espace métrique compact et F espace métrique complet.

On a : $\mathcal{A}$ relativement compacte dans $\mathcal{C}(K,F)$ ssi

$$\begin{cases} (i) & \mathcal{A} \text{ est équicontinue sur } K \\ (ii) & \text{pour tout } x \text{ dans } K,\ \mathcal{A}(x) = \{f(x) : f \in \mathcal{A}\} \text{ est relativement compacte dans } F \end{cases}$$

preuve :

Supposons que $\mathcal{A}$ est relativement compacte dans $\mathcal{C}(K,F)$.

Montrons (i) : Soit $\varepsilon > 0$, soit $B(f_j, \varepsilon)$ $(1 \leq j \leq k)$ tel que $\mathcal{A} \subseteq \bigcup_{j=1}^{k} B(f_j, \varepsilon)$ où $f_j \in \mathcal{A}$.

Soit η tel que $\forall 1 \leq j \leq k, \forall x, y \in E, d(x,y) < \eta \Rightarrow d(f_j(x), f_j(y)) < \varepsilon$ (ce η vient de l'uniforme continuité des f_j sur K qui est compact).

Soit f dans $\mathcal{A}$ quelconque, soit j tel que $d_\infty(f, f_j) < \varepsilon$, on a donc :

$$\forall x, y \in K, d(x,y) < \eta \Rightarrow d(f(x), f(y)) \leq d(f(x), f_j(x)) + d(f_j(x), f_j(y)) + d(f_j(y), f(y)) < 3\varepsilon$$

Montrons (ii) : Soit x dans K, soit $(y_n)_n \in (\mathcal{A}(x))^{\mathbb{N}}$, on écrit $y_n = f_n(x)$ avec $f_n \in \mathcal{A}$, par relative compacité, on peut extraire une sous-suite $(f_{\phi(n)})_n$ qui converge vers $f \in \mathcal{C}(K,F)$ (pour la topologie de $\mathcal{C}(K,F)$ ie convergence uniforme), alors $(y_{\phi(n)})$ converge vers $f(x) \in F$.

Supposons (i) et (ii), et montrons que $\mathcal{A}$ est relativement compacte.

Soit $(f_n)_n \in (\mathcal{A})^{\mathbb{N}}$, montrons qu'elle admet une sous-suite convergeante.

Soit $D = \{d_k : k \in \mathbb{N}\}$ un ensemble dénombrable dense dans K.

Montrons qu'il existe une sous-suite $(f_{\varphi(n)})_n$ qui converge simplement sur D

La suite $(f_n(d_0))_n$ est à valeurs dans $\mathcal{A}(d_0)$ qui est relativement compact, il existe donc φ_0 tel que $f_{\varphi_0(n)(d_0)}$ converge vers une limite notée $f(d_0)$.

En appliquant le même raisonnement à $(f_{\varphi_0(n)(d_1)})_n$, on en déduit l'existence de φ_1 tel que $(f_{\varphi_0\circ\varphi_1(n)(d_1)})_n$ converge vers une limite $f(d_1)$.

En itérant ce procédé, on construit par récurrence une suite d'extractrice $(\varphi_n)_n$ tel que $\forall k, f_{\varphi_0\circ\cdots\circ\varphi_k(n)}(d_k)$ converge vers $f(d_k)$

Soit $\varphi(n) = \varphi_0 \circ \cdots \circ \varphi_n(n)$ (extraction diagonale). On a alors :

$$\forall k, \forall n \geq k, f_{\varphi(n)}(d_k) = f_{\varphi_0\circ\cdots\circ\varphi_k(\varphi_{k+1}\circ\cdots\circ\varphi_n(n))}(d_k) \longrightarrow f(d_k)$$

puisque c'est une sous-suite de $f_{\varphi_0\circ\cdots\circ\varphi_k(n)}(d_k)$.

On a donc bien que $(f_{\varphi(n)})_n$ converge simplement sur D vers une certaine fonction f définie sur D.

Montrons que f est uniformément continue sur D

Soit $\varepsilon > 0$, soit η tel que $\forall x, y \in K, d(x,y) < \eta \Rightarrow \forall g \in \mathcal{A}, d(g(x), g(y)) < \varepsilon$ (par (i))

Soient $x, y \in K$ tels que $d(x,y) < \eta$, soient $n_\varepsilon \in \mathbb{N}$ tel que $d(f_{\varphi(n_\varepsilon)}(x), f(x)) < \varepsilon$ et $d(f_{\varphi(n_\varepsilon)}(y), f(y)) < \varepsilon$.

On a alors : $d(f(x), f(y)) \leq d(f(x), f_{\varphi(n_\varepsilon)}(x)) + d(f_{\varphi(n_\varepsilon)}(x), f_{\varphi(n_\varepsilon)}(y)) + d(f_{\varphi(n_\varepsilon)}(y), f(y)) < 3\varepsilon$

Donc f est uniformément continue sur D, et peut donc se prolonger sur K (car F est complet). Ce prolongement est de plus uniformément continue. On notera toujours f ce prolongement.

Montrons que $(f_{\varphi(n)})_n$ converge uniformément sur K vers f

Soit $\varepsilon > 0$, soit $\eta > 0$ défini par l'uniforme équicontinuité de $\mathcal{A}$ sur K et par l'uniforme continuité de f sur K.

Soit $K \subseteq \bigcup_{j=1}^{k} B(x_j, \eta)$ un recouvrement de K, où $\forall j, x_j \in D$.

Soit n_ε tel que $\forall j, \forall n \geq n_\varepsilon, d(f(x_j), f_n(x_j)) < \varepsilon$. Pour tout $n \geq n_\varepsilon$, pour tout $x \in K$, soit j tel que $d(x, x_j) < \eta$. On a alors :

$$d(f(x), f_{\varphi(n)}(x)) \leq d(f(x), f(x_j)) + d(f(x_j), f_{\varphi(n)}(x_j)) + d(f_{\varphi(n)}(x_j), f_{\varphi(n)}(x)) < 3\varepsilon$$

■

Conséquences du Théorème d'Ascoli :

- le théorème de Cauchy-Arzela (par la méthode d'Euler)
- si une suite de fonctions équicontinues $(f_n)_n$ définies sur un compact K converge simplement sur K, alors la convergence est uniforme.
- démontrer que l'opérateur $T : f \in \mathcal{C}([a,b], \mathbb{R}) \longmapsto \int_a^b K(x,y)f(y)dy$ où $K \in \mathcal{C}([a,b] \times [a,b], \mathbb{R})$ est compact

2.3 Théorème d'inversion locale

Références *: [Rouvière,] p.222*

Lemme :

Soit $u : \mathbb{R}^n \to \mathbb{R}^n$ une application linéaire. Soit $\|.\|$ une norme sur $\mathbb{R}^n$ subordonnée à une norme de $\mathbb{R}^n$. Si on suppose que $\|u\| < 1$, alors $Id - u$ est inversible, d'inverse $(Id-u)^{-1} = \sum_{k=0}^{\infty} u^k$

Théorème :

Soit U un ouvert de $\mathbb{R}^n$ qui contient 0. Soit $f : U \to \mathbb{R}^n$ de classe $\mathcal{C}^1$ telle que $f(0) = 0$ et telle que $df(0)$ est inversible.

Alors : il existe V, W ouverts de $\mathbb{R}^n$ contenant 0 tels que f induit un $\mathcal{C}^1-$difféomorphisme de V sur W.

preuve :

Pour $y \in \mathbb{R}^n$, posons $F_y : x \in U \mapsto x + df(0)^{-1}(y - f(x))$

Pour $r > 0$, soient $B_r = \{x \in \mathbb{R}^n : \|x\| < r\}$ et $\overline{B_r} = \{x \in \mathbb{R}^n : \|x\| \leq r\}$

Montrons qu'il existe $r > 0$ tel que : $\forall y \in \mathbb{R}^n, \forall x \in B_r \cap U, \|dF_y(x)\| \leq \frac{1}{2}$

Soit $y \in \mathbb{R}^n$. On sait que F_y est $\mathcal{C}^1$ sur U et on a :

$$\forall x \in U, dF_y(x) = Id - df(0)^{-1}(df(x))$$

Donc $dF_y(0) = 0$, et par continuité de $x \mapsto dF_y(x)$ (puisque F_y est $\mathcal{C}^1$), on sait qu'il existe $r > 0$ tel que : $\forall x \in B_r \cap U, \|dF_y(x)\| \leq \frac{1}{2}$.

De plus, le r qu'on a choisit ne dépend pas de y puisque dF_y ne dépend pas non plus de y.

Remarque : quitte à réduire r, on peut supposer que $\overline{B_r} \subseteq U$. On fait cette hypothèse dans la suite.

Posons $W = \left\{y \in \mathbb{R}^n : \|df(0)^{-1}(y)\| < \frac{r}{2}\right\}$

Montrons que : $\forall y \in W, F_y\left(\overline{B_r}\right) \subseteq B_r$

Soit $y \in W$. Soit $x \in \overline{B_r}$.

On a : $\|F_y(x)\| \leq \|F_y(x) - F_y(0)\| + \|F_y(0)\|$

Par ailleurs, $\|F_y(0)\| = \|df(0)^{-1}(y)\| < \frac{r}{2}$ (puisque $y \in W$).

Et, par l'inégalité des accroissements finis, on a : $\|F_y(x) - F_y(0)\| \leq \frac{1}{2}\|X\| \leq \frac{r}{2}$

D'où $\|F_y(x)\| < r$

Posons $V = B_r \cap f^{-1}(W)$

Montrons que f induit une bijection de V sur W

On a :

$$\begin{aligned} f : V \to W \text{ bijective} &\Leftrightarrow \forall y \in W, \exists! x \in V, y = f(x) \\ &\Leftrightarrow \forall y \in W, \exists! x \in V, F_y(x) = x \\ &\Leftrightarrow \forall y \in W, F_y \text{ admet un unique point fixe sur } V \end{aligned}$$

Soit $y \in W$. Comme $F_y : \overline{B_r} \to \overline{B_r}$ est contractante (par l'inégalité des accroissements finis), on sait que F_y admet un unique point fixe $x \in \overline{B_r} \supseteq V$. Il suffit alors de montrer que ce x appartient à V (ie $x \in B_r$ et $x \in f^{-1}(W)$). Ceci est clair, puisque $x = F_y(x) \in B_r$ (puisque $F_y(\overline{B_r}) \subseteq B_r$) et que $y = f(x)$ (puisque $F_y(x) = x$).

Montrons que f^{-1} est lipschitzienne sur W

Soient $y_1, y_2 \in W$, soient $x_1, x_2 \in V$ tels que $y_i = f(x_i)$ $(1 \leq i \leq 2)$. On a :

$$\begin{aligned} x_1 - x_2 &= F_{y_1}(x_1) - F_{y_2}(x_2) \\ &= (F_{y_1}(x_1) - F_{y_1}(x_2)) + (F_{y_1}(x_2) - F_{y_2}(x_2)) \qquad = (F_{y_1}(x_1) - F_{y_1}(x_2)) + df(0)^{-1}(y_1 - y_2) \end{aligned}$$

Par l'inégalité des accroissements finis :

$$\|x_1 - x_2\| \leq \frac{1}{2}\|x_1 - x_2\| + \|df(0)^{-1}\|.\|y_1 - y_2\|$$

D'où

$$\frac{1}{2}\|x_1 - x_2\| \leq \|df(0)^{-1}\|.\|y_1 - y_2\|$$

Autrement dit

$$\forall y_1, y_2 \in W, \|f^{-1}(y_1) - f^{-1}(y_2)\| \leq 2\|df(0)^{-1}\|.\|y_1 - y_2\|$$

Donc f^{-1} est lipschitzienne sur W, donc continue sur W.

Montrons que $\forall x \in B_r, df(x)$ inversible

Soit $x \in B_r$. Soit $y \in W$ quelconque. On a donc $\|dF_y(x)\| \leq \frac{1}{2}$. Par le lemme, on sait donc que la somme $\sum_{k=0}^{\infty} (dF_y(x))^k$ converge, et est inversible d'inverse $Id - dF_y(x)$. Au début de la preuve on avait calculer que $Id - dF_y(x) = df(0)^{-1}(df(x))$. On sait donc que $df(x)$ est inversible.

Montrons que f^{-1} est $\mathcal{C}^1$ sur W

Soient $y, y_0 \in W$, soient $x, x_0 \in V$ tels que $y = f(x)$ et $y_0 = f(x_0)$. On a :

$$y - y_0 = f(x) - f(x_0) = df(x_0)(x - x_0) + R$$

Avec $R = o(\|x - x_0\|)$.

Et, comme $\|x - x_0\| \leq C.\|y - y_0\|$ où C est une constante (on a déjà montré que f^{-1} est lipschitzienne), on sait que R est aussi un $o(\|y - y_0\|)$.

On peut donc écrire :

$$df(x_0)(x - x_0) = y - y_0 + o(\|y - y_0\|)$$

Autrement dit

$$f^{-1}(y) - f^{-1}(y_0) = df(x_0)^{-1}(y - y_0) + o(\|y - y_0\|)$$

ie

$$f^{-1}(y) - f^{-1}(y_0) = df(f^{-1}(y_0))^{-1}(y - y_0) + o(\|y - y_0\|)$$

Donc f^{-1} est différentiable, et $d(f^{-1})(y) = df(f^{-1}(y))^{-1}$

De plus, comme $y \mapsto d(f^{-1})(y)$ est la composée de trois foncions continue, on sait que f est $\mathcal{C}^1$.

■

2.4 Développement asymptotique d'une intégrale

Références : *[Rouvière,] p.245*

Soient $a < b$.

Soit $f : \begin{cases} \mathbb{R}\times\mathbb{R} & \longrightarrow & \mathbb{R} \\ (x,\varepsilon) & \longmapsto & \varepsilon x^3 + (x-a)(b-x) \end{cases}$

Proposition :

Pour $\varepsilon > 0$ assez petit, l'équation $f(x,\varepsilon) = 0$ a trois solutions distinctes $x_1(\varepsilon) < x_2(\varepsilon) < x_3(\varepsilon)$. De plus, on a :

- $x_1(\varepsilon) = a - \frac{a^3}{b-a}\varepsilon + O(\varepsilon^2)$
- $x_2(\varepsilon) = b + \frac{b^3}{b-a}\varepsilon + O(\varepsilon^2)$
- $x_3(\varepsilon) = \frac{1}{\varepsilon} - (a+b) - (a^2+ab+b^2)\varepsilon + O(\varepsilon^2)$

preuve :

On a $f(a,0) = 0$, et $\frac{\partial f}{\partial x}(x,\varepsilon) = 3\varepsilon x^2 - 2x + a + b$. Donc $\frac{\partial f}{\partial x}(a,0) = b - a > 0$.

Par le théorème des fonctions implicites, on sait qu'il existe un intervalle ouvert V_1 de 0 et un voisinage W_1 de a tels que $\forall \varepsilon \in V_1, f(x_1(\varepsilon),\varepsilon) = 0$. De plus, on sait que la fonction implicite x_1 est $\mathcal{C}^2$ (et même $\mathcal{C}^\infty$), puisque f l'est. Par l'inégalité de Taylor-Lagrange à l'ordre 2, on a donc :

$$\forall \varepsilon \in V_1, x_1(\varepsilon) = a + \varepsilon x_1'(0) + O(\varepsilon^2)$$

Or, on sait que $\forall \varepsilon \in V_1, \varepsilon x_1(\varepsilon)^3 - x_1(\varepsilon)^2 + (a+b)x_1(\varepsilon) - ab = f(x_1(\varepsilon),\varepsilon) = 0$

En dérivant, on obtient : $\forall \varepsilon \in V_1, x_1(\varepsilon)^3 + 3_1'(\varepsilon)x_1(\varepsilon)^2 - 2x_1'(\varepsilon)x_1(\varepsilon) + (a+b)x_1'(\varepsilon) = 0$

En prenant $\varepsilon = 0$, on obtient : $a^3 - 2x_1'(0)a + (a+b)x_1'(0) = 0$

On a donc : $x_1'(0) = -\frac{a^3}{b-a}$

D'où $\forall \varepsilon \in V_1, x_1(\varepsilon) = a - \frac{a^3}{b-a}\varepsilon + O(\varepsilon^2)$

De même, on trouve une fonction implicite x_2 d'un intervalle ouvert V_2 de b dans un voisinage W_2 de 0 telle que $\forall \varepsilon \in V_2, f(x_2(\varepsilon),\varepsilon) = 0$.

Avec le même raisonnement, on trouve : $\forall \varepsilon \in V_2, x_2(\varepsilon) = b + \frac{b^3}{b-a}\varepsilon + O(\varepsilon^2)$

Les relations racines-coefficients donne l'existence d'une $x_3 : V = V_1 \cap V_2 \to \mathbb{R}$ qui vérifie :

$$\forall \varepsilon \in V, x_1(\varepsilon) + x_2(\varepsilon) + x_3(\varepsilon) = \frac{1}{\varepsilon}$$

D'où : $\forall \varepsilon \in V, x_3(\varepsilon) = \frac{1}{\varepsilon} - (a+b) - (a^2+ab+b^2)\varepsilon + O(\varepsilon^2)$ ■

Proposition :

Pour ε assez petit, on définit $I(\varepsilon) = \displaystyle\int_{x_1(\varepsilon)}^{x_2(\varepsilon)} \frac{1}{\sqrt{f(x,\varepsilon)}}dx$

Pour ε assez petit, $I(\varepsilon) = \pi + \frac{3\pi}{4}(a+b)\varepsilon + O(\varepsilon^2)$

preuve :

On a : $f(x,\varepsilon) = \varepsilon(x - x_1(\varepsilon))(x_2(\varepsilon) - x)(x_3(\varepsilon) - x) = (x - x_1)(x_2 - x)(1 - \varepsilon(x + x_1 + x_2))$

Rq : On écrit x_1 au lieu de $x_1(\varepsilon)$ pour alléger les notations.

D'où

$$I(\varepsilon) = \int_{x_1}^{x_2} \frac{(1 - \varepsilon(x + x_1 + x_2))^{-1/2}}{\sqrt{(x - x_1)(x - x_2)}} dx$$

En faisant le changement de variables $x = u + v\sin t$ avec $u = \frac{x_1+x_2}{2}$ et $v = \frac{x_2-x_1}{2}$, on a :

$$I(\varepsilon) = \int_{-\pi/2}^{\pi/2} (1 - \varepsilon(3u + v\sin t))^{-1/2} dt \tag{1}$$

Notons $y = 3u + v\sin t$. Comme $x_1 = a + O(\varepsilon)$ et $x_2 = b + O(\varepsilon)$, on a

$$y = \frac{3}{2}(a + b) + \frac{b - a}{2}\sin t + O(\varepsilon) \tag{2}$$

Rq : le dernier grand $O(\varepsilon)$ est uniforme en t, puisque $|\sin t| \leq 1, \forall t$.

D'autre part,

$$(1 - \varepsilon y)^{-1/2} = 1 + \frac{\varepsilon}{2} y + O(\varepsilon) \tag{3}$$

Rq : ce grand $O(\varepsilon)$ est aussi uniforme en t, puisque $|\sin t| \leq 1, \forall t$.

En injectant (2) et (3) dans (1), et parceque les $O(\varepsilon)$ sont uniformes en t, on a :

$$I(\varepsilon) = \int_{-\pi/2}^{\pi/2} \left(1 + \frac{3}{4}(a + b)\varepsilon + \frac{b - a}{4}\varepsilon\sin t\right) dt + O(\varepsilon^2)$$

D'où $I(\varepsilon) = \pi + \frac{3\pi}{4}(a + b)\varepsilon + O(\varepsilon^2)$

■

2.5 Méthode du gradient à pas optimal

Références : *[Francinou* et al., *g] p.39*

Lemme :

Soit $f : \mathbb{R}^n \longrightarrow \mathbb{R}$ continue telle que $\lim_{\|x\|\to\infty} f(x) \longrightarrow +\infty$. Alors f admet un minimum.

preuve :

Soit $A > 0$ tel que, $\forall x, \|x\| > A \Rightarrow f(x) > f(0)$.

La boule de centre 0 et de rayon A est un compact de $\mathbb{R}^n$. Soit donc a un point de cette boule où la restriction de f à la boule atteint son minimum.

On a alors, $\forall x \in B(0, A), f(x) \geq f(a)$

Et $\forall x \in \mathbb{R}^n \backslash B(0, A), f(x) > f(0) \geq f(a)$

Donc f admet bien un minimum en a.

■

Soit $G : \mathbb{R}^n \longrightarrow \mathbb{R}$ $\mathcal{C}^1$ et $\alpha > 0$ tels que :

$$\forall x, y \in \mathbb{R}^n, G(y) - G(x) \geq \langle \text{grad}_G(x), y - x \rangle + \alpha \|y - x\|^2$$

Proposition :

G atteint sa borne inférieure en un unique point $a \in \mathbb{R}^n$.

De plus, $\forall x \in \mathbb{R}^n, \text{grad}_G(x) = 0 \Rightarrow x = a$

preuve :

Montrons que G admet un minimum en un point a

On a : $\forall y, G(y) \geq G(0) + \langle \text{grad}_G(0), y \rangle + \alpha \|y\|^2 = O(\|y\|) + \alpha \|y\|^2 \underset{\|y\|\to+\infty}{\longrightarrow} +\infty$ (cf l'inégalité de Cauchy-Schwarz)

Donc le lemme donne l'existence d'un point a en lequel G est minimale.

Montrons que $\forall x, \textbf{grad}_G(x) = 0 \Rightarrow x = a$

Supposons que $\text{grad}_G(x) = 0$ pour un certain $x \in \mathbb{R}^n$.

Alors, on a : $G(a) - G(x) \geq \langle \text{grad}_G(x), a - x \rangle + \alpha \|x - a\|^2$

D'où : $G(x) \leq G(a) - \|x - a\|^2$

Par minimalité de $G(a)$, on a nécessairement $\|x - a\|^2 = 0$

D'où $x = a$.

La propriété que l'on vient de démontrer donne aussi l'unicité du point en lequel G atteint son minimum, puisque tout point définissant un extremum global de G définit un extremum local (G est défini sur $\mathbb{R}^n$), donc est un point critique.

■

Proposition :

Soit $(x_k)_k \in (\mathbb{R}^n)^{\mathbb{N}}$ définie par un $x_0 \in \mathbb{R}^n$ et pour tout k, x_{k+1} est un point de $x_k + \mathbb{R}\text{grad}_G(x_k)$ qui minimise la restriction de G.

Alors $(x_k)_k$ converge vers a.

preuve :

Montrons que la suite $(x_k)_k$ est bien définie

Supposons que x_k soit construit.

Si $\text{grad}_G(x_k) = 0$, alors on a $x_k = a$, et on pose $x_{k+1} = a$.

Sinon, on pose $\varphi_{x_k} : t \in \mathbb{R} \longmapsto G(x_k + t\text{grad}_G(x_k))$

φ_{x_k} est continue, et $\varphi_{x_k}(t) \underset{|t|\to+\infty}{\longrightarrow} +\infty$, donc par le lemme, on peut définir t_k comme un point où φ_{x_k} atteint son minimum, puis poser $x_{k+1} = x_k + t_k\text{grad}_G(x_k)$.

Montrons que $\forall k, \langle \mathbf{grad}_G(x_k), \mathbf{grad}_G(x_{k+1})\rangle = 0$

Si $\text{grad}_G(x_k) = 0$, le résultat est évident.

Sinon, on sait que t_k définit un extremum global de φ_{x_k}, donc aussi un extremum local, donc est un point critique.

Par ailleurs, $\forall t, \varphi'_{x_k}(t) = \langle \text{grad}_G(x + t\text{grad}_G(x_k)), \text{grad}_G(x_k)\rangle$

D'où $0 = \varphi'_{x_k}(t_k) = \langle \text{grad}_G(x_{k+1}), \text{grad}_G(x_k)\rangle$

Montrons que $(x_k)_k$ converge vers a

Par construction $(G(x_k))_k$ est décroissante et minorée par $G(a)$, donc admet une limite $l \in \mathbb{R}$. En particulier, $(G(x_k))$ est bornée.

Comme $G(x) \underset{\|x\|\to+\infty}{\longrightarrow} +\infty$, on sait que $(x_k)_k$ est aussi bornée. On va montrer que a est son unique valeur d'adhérence. Soit donc b une valeur d'adhérence de $(x_k)_k$, soit ψ une extractrice telle que $x_{\psi(k)} \to b$.

On a : $\alpha\|x_{\psi(k)} - x_{\psi(k)+1}\|^2 \leq G(x_{\psi(k)}) - G(x_{\psi(k)+1}) \to 0$. Donc $(x_{\psi(k)+1})_k$ converge aussi vers b.

Par ailleurs, on a : $\forall k, 0 = \left\langle \text{grad}_G(x_{\psi(k)}), \text{grad}_G(x_{\psi(k)+1})\right\rangle \to \langle \text{grad}_G(b), \text{grad}_G(b)\rangle = \|\text{grad}_G(b)\|^2$

Donc $\text{grad}_G(b) = 0$, et $b = a$.

■

2.6 Inégalités de Kolmogorov

Références : *[Francinou* et al.*, d] p.274*

Proposition :

Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$ $\mathcal{C}^2$. Soit $M_k = \sup_{x\in\mathbb{R}} f^{(k)}(x)$ $(0 \leq k \leq 2)$. On suppose que $M_0, M_2 < +\infty$.

Alors : $M_1 \leq \sqrt{2M_0M_2}$

preuve :

Soit $x \in \mathbb{R}$.

Pour $h > 0$, on écrit l'inégalité de Taylor-Lagrange entre x et $x+h$, et entre x et $x-h$.

$$\forall h > 0, |f(x+h) - f(x) - hf'(x)| \leq \frac{h^2}{2} M_2$$

$$\forall h > 0, |f(x-h) - f(x) + hf'(x)| \leq \frac{h^2}{2} M_2$$

D'autre part, en utilisant l'inégalité triangulaire, on a :

$$\forall h > 0, 2h|f'(x)| = |(f(x-h) - f(x) + hf'(x)) + (-f(x+h) + f(x) + hf'(x)) - f(x-h) + f(x+h)| \leq h^2 M_2 + 2M_0$$

D'où : $\forall h > 0, |f'(x)| \leq \frac{hM_2}{2} + \frac{M_0}{h}$

En particulier, si on prend $h = \sqrt{2\frac{M_0}{M_2}}$, on obtient :

$|f'x)| \leq \sqrt{2M_0M_2}$

Ceci étant vrai pour tout $x \in \mathbb{R}$, on a bien $M_1 \leq \sqrt{2M_0M_2}$.

■

Proposition :

Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$ $\mathcal{C}^n$ $(n \in \mathbb{N}^*)$. Pour toute fonction g $\mathcal{C}^m$, on notera $M_k(g) = \sup_{x\in\mathbb{R}} g^{(k)}(x)$ $(0 \leq k \leq m)$. On notera $M_k = M_k(f)$. On suppose $M_0, M_n < +\infty$.

Alors $\forall k \in [\![0, n]\!], M_k \leq 2^{k(n-k)/2} M_0^{1-k/n} M_n^{k/n}$

preuve :

D'abord, montrons que tous les M_k sont finis

Soit $x \in \mathbb{R}$. Soient $0 < h_0 < \cdots < h_{n-1}$

On a :

$$\forall 0 \leq j \leq n-1, |f(x+h_j) - f(x) - h_j f'(x) - \cdots - \frac{h_j^{n-1}}{(n-1)!} f^{(n-1)}(x)| \leq \frac{h_j^n}{n!} M_n$$

D'où (par l'inégalité triangulaire) :

$$\forall 0 \leq j \leq n-1, |f(x) + h_j f'(x) + \cdots + \frac{h_j^{(n-1)}}{(n-1)!} f^{(n-1)}(x)| \leq M_0 + \frac{h_j^n}{n!} M_n \leq M_0 + \frac{h_{n-1}^n}{n!} M_n = K < +\infty$$

Autrement dit :

$$\left\| \begin{pmatrix} f(x) + h_0 f'(x) + \cdots + \frac{h_0^{n-1}}{(n-1)!} f^{(n-1)}(x) \\ \vdots \\ f(x) + h_{n-1} f'(x) + \cdots + \frac{h_{n-1}^{n-1}}{(n-1)!} f^{(n-1)}(x) \end{pmatrix} \right\|_\infty \leq K$$

Donc :

$$\left\| \underbrace{\begin{pmatrix} 1 & h_0 & \cdots & \frac{h_0^{n-1}}{(n-1)!} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & h_{n-1} & \cdots & \frac{h_{n-1}^{n-1}}{(n-1)!} \end{pmatrix}}_{V} \underbrace{\begin{pmatrix} f(x) \\ \vdots \\ f^{(n-1)}(x) \end{pmatrix}}_{F(x)} \right\|_\infty \leq K$$

Or V est inversible. En effet, $\det V = \frac{1}{2! \cdots (n-1)!} \prod_{i<j} (h_j - h_i) > 0$ (cf déterminant de Vandermonde).

En notant $\|.\|$ la norme subordonnée à $\|.\|_\infty$, on a :

$$\|F(x)\|_\infty = \|V^{-1}(V.F(x))\|_\infty \leq \|V^{-1}\|.K$$

Ceci étant vrai pour tout $x \in \mathbb{R}$, on a : $\forall k \in [\![0, n]\!], M_k \leq \|V^{-1}\|.K < +\infty$

Montrons maintenant l'inégalité

On va procéder par récurrence sur n. Le cas $n = 2$ a déjà été fait dans la proposition précédente.

Soit $f : \mathbb{R} \longrightarrow \mathbb{C}$ $\mathcal{C}^{n+1}$.

On suppose que $\forall g : \mathbb{R} \longrightarrow \mathbb{C}$ $\mathcal{C}^m$, si $m \leq n$ et que $M_0(g), M_m(g) < +\infty$, alors

$$\forall 0 \leq i \leq m, M_i(g) \leq 2^{i(m-i)/2} M_0(g)^{1-i/m} M_m(g)^{i/m}$$

On suppose de plus que $M_0, M_{n+1} < +\infty$. On vient de démontrer que $\forall 0 \leq k \leq n+1, M_k < +\infty$.

Soit $k \in [\![1, n]\!]$.

Appliquons le cas $n = 2$ à $f^{(k-1)}$ (qui est bien $\mathcal{C}^2$) :

$$M_1\left(f^{(k-1)}\right)^2 \leq 2 M_0\left(f^{(k-1)}\right) M_2\left(f^{(k-1)}\right)$$

Autrement dit,

$$M_k^2 \leq 2 M_{k-1} M_{k+1} \tag{1}$$

En appliquant l'hypothèse de récurrence à $g = f$, $m = k$ et $i = k - 1$, on a :

$$M_{k-1}(f) \leq 2^{(k-1)/2} M_0(f)^{1-(k-1)/k} M_k(f)^{(k-1)/k}$$

Autrement dit,

$$M_{k-1} \leq 2^{(k-1)/2} M_0^{1/k} M_k^{1-1/k} \tag{2}$$

En appliquant l'hypothèse de récurrence à $g = f^{(k)}$, $m = n + 1 - k$ et $i = 1$, on a :

$$M_1\left(f^{(k)}\right) \leq 2^{(n-k)/2} M_0\left(f^{(k)}\right)^{1-1/(n+1-k)} M_{n+1-k}\left(f^{(k)}\right)^{1/(n+1-k)}$$

Autrement dit,

$$M_{k+1} \leq 2^{(n-k)/2} M_k^{1-1/(n+1-k)} M_{n+1}^{1/(n+1-k)} \tag{3}$$

En injectant les inégalités (2) et (3) dans (1), on a :

$$M_k^2 \leq 2^{(n+1)/2} M_0^{1/k} M_k^{(k-1)/k+(n-k)/(n+1-k)} M_{n+1}^{1/(n+1-k)}$$

En élevant à la puissance $\frac{k(n+1-k)}{n+1}$, on a bien :

$$M_k \leq 2^{k(n+1-k)/2} M_0^{1-k/(n+1)} M_{n+1}^{k/(n+1)}$$

■

2.7 Equation de Bessel

Références : *[Francinou* et al.*, g] p.101*

On considère l'équation différentielle :

$$xy'' + y' + xy = 0 \tag{E}$$

Proposition :

$g : x \mapsto \frac{1}{\pi}\int_0^\pi \cos(x\sin\theta)d\theta$ est solution de (E).

preuve :

La fonction $(x,\theta) \mapsto \cos(x\sin\theta)$ est $\mathcal{C}^\infty$, donc par le théorème de dérivation sous l'intégrale (on intègre sur un segment), on sait que g est aussi $\mathcal{C}^\infty$, et on a :

$$g'(x) = -\frac{1}{\pi}\int_0^\pi \sin(x\sin\theta)\sin\theta d\theta$$

$$g''(x) = -\frac{1}{\pi}\int_0^\pi \cos(x\sin\theta)(\sin\theta)^2 d\theta$$

On a donc, pour tout $x \in \mathbb{R}$,

$$\begin{aligned} xg''(x) + g'(x) + xg(x) &= \frac{1}{\pi}\int_0^\pi \left(x\cos(x\sin\theta)(1-(\sin\theta)^2) - \sin(x\sin\theta)\sin\theta\right)d\theta \\ &= \frac{1}{\pi}\int_0^\pi \left(x\cos(x\sin\theta)(\cos\theta)^2 - \sin(x\sin\theta)\sin\theta\right)d\theta \\ &= \frac{1}{\pi}\left[\sin(x\sin\theta)\cos\theta\right]_0^\pi \\ &= 0 \end{aligned}$$

■

Proposition :

Les solutions de (E) développables en série entière sont exactement les fonctions de la forme $x \mapsto \lambda \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n(n!)^2}x^{2n}$ avec $\lambda \in \mathbb{R}$.

preuve :

Soit f une solution de (E) développable en série entière au voisinage de 0. Soient $(a_n)_n \in \mathbb{R}^{\mathbb{N}}$ et $R > 0$ tels que :

$$\forall x \in]-R,R[, f(x) = \sum_{n=0}^{\infty} a_n x^n$$

On sait alors que :

$$\forall x \in]-R,R[, xf(x) = \sum_{n=0}^{\infty} a_n x^{n+1} = \sum_{n=1}^{\infty} a_{n-1}x^n$$

$$\forall x \in]-R,R[, f'(x) = \sum_{n=1}^{\infty} n a_n x^{n-1} = \sum_{n=0}^{\infty} (n+1)a_{n+1}x^n$$

$$\forall x \in]-R,R[, xf''(x) = \sum_{n=2}^{\infty} n(n-1)a_n x^{n-1} = \sum_{n=1}^{\infty} n(n+1)a_{n+1}x^n$$

Comme f est solution de (E), on a :

$$\forall x \in]-R,R[, 0 = xf''(x) + f'(x) + xf(x) = a_1 + \sum_{n=1}^{\infty} (a_{n-1} + (n+1)a_{n+1} + n(n+1)a_{n+1})x^n$$

Donc :

$$\begin{cases} a_1 = 0 \\ \forall n \in \mathbb{N}^*, a_{n-1} + (n+1)^2 a_{n+1} = 0 \end{cases}$$

Donc, avec une récurrence immédiate, on en déduit que $\forall n \in \mathbb{N}^*, a_{2n+1} = 0$ et que $\forall n \in \mathbb{N}^*, a_{2n} = \frac{(-1)^n}{4^n (n!)^2} a_0$.

On a donc, $\forall x \in]-R,R[, f(x) = a_0 \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n (n!)^2} x^{2n}$.

Réciproquement, cette série entière a un rayon de convergence infini, et donc est bien une solution de (E) sur $\mathbb{R}$. ■

Soit $f_0 : x \mapsto \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n (n!)^2} x^{2n}$

Proposition :

Soit f une solution de (E) définie sur $]0,\infty[$. Alors : (f, f_0) est libre ssi f non-bornée au voisinage de 0.

preuve :

La fonction f_0 est continue en 0, donc bornée au voisinage de 0.

Il est alors clair que si (f, f_0) est liée, alors f est aussi bornée au voisinage de 0.

Supposons que (f, f_0) est libre, et montrons que f n'est pas bornée au voisinage de 0

Sur $\mathbb{R}_+^*$, (E) s'écrit sous forme résolue $y'' + \frac{1}{x}y' + y = 0$, les solutions de (E) sur R_+^* forment donc un espace vectoriel de dimension 2, dont (f, f_0) est une base. Soit $W = f.f_0' - f_0.f'$ le wronskien associé à cette base.

On a :

$$\begin{aligned} \forall x > 0, W'(x) &= f(x).f_0''(x) - f_0(x).f''(x) \\ &= f(x)(-\frac{1}{x}f_0'(x) - f_0(x)) + f_0(x)(\frac{1}{x}f'(x) + f(x)) \\ &= -\frac{1}{x}W(x) \end{aligned}$$

On sait alors, qu'il existe $C \in \mathbb{R}$ tel que $\forall x > 0, W(x) = \frac{C}{x}$

On sait que $C \neq 0$, puisque la famille (f, f_0) est libre.

On a donc : $\forall x > 0, f(x)f_0'(x) - f'(x)f_0(x) = \frac{C}{x}$

Si f était bornée au voisinage de 0, alors, comme $f_0(x) \underset{x\to 0}{\to} 1$ et que $f_0(x) \underset{x\to 0}{\to} 0$, on aurait (en faisant tendre x vers 0 dans l'égalité précédente) :

$$f'(x) \underset{x\to 0}{\sim} -\frac{C}{x}$$

Mais, comme $x \mapsto -\frac{C}{x}$ garde un signe constant, et n'est pas intégrable sur $]0,1]$, on aurait aussi :

$$f(1) - f(x) = \int_x^1 f'(t)dt \underset{x\to 0}{\sim} -C\int_x^1 \frac{dt}{t} = C\ln x$$

On aurait alors : $f(x) \underset{x\to 0}{\sim} -C\ln x$ qui n'est pas bornée au voisinage de 0.

On sait donc que, sous l'hypothèse que (f, f_0) est libre, f n'est pas bornée au voisinage de 0.

■

Proposition :

$$\forall x \in \mathbb{R}, \frac{1}{\pi}\int_0^{\pi} \cos(x\sin\theta)d\theta = \sum_{n=0}^{\infty} \frac{(-1)^n}{4^n(n!)^2}x^{2n}$$

preuve :

La fonction g (introduit dans la première proposition) est bornée sur $\mathbb{R}$, donc la famille (f_0, g) est liée sur $]0,\infty[$. Par continuité en 0, (f_0, g) est liée sur $\mathbb{R}_+$. Et, comme $f_0(0) = 1 = g(0)$, on sait que $\forall x \geq 0, f_0(x) = g(x)$. Comme f_0 et g sont paires, on en déduit que $\forall x \in \mathbb{R}, g(x) = f_0(x)$ ■

2.8 Problème de Cauchy avec conditions aux limites

Références *: [Francinou* et al.*, g] p.112*

Soit $p : \mathbb{R}^+ \to \mathbb{R}$ continue telle que $\int_0^\infty t|p(t)|dt < \infty$

L'équation différentielle $y'' + py = 0$ admet une unique solution telle que $\lim_\infty y = 1$ et $\lim_\infty y' = 0$.

Procédons par analyse–synthèse. Soit y une telle solution. On sait que y est bornée (en effet, y est continue et admet une limite finie en ∞).

On a : $\forall x \in \mathbb{R}^+, y(x) = 1 - \int_x^\infty y'(t)dt$ (puisque $\lim_\infty y = 1$).

En intégrant par paties : $\forall x \in \mathbb{R}^+, y(x) = 1 - [(t-x)y'(t)]_x^\infty + \int_x \infty(t-x)y''(t)dt$

Comme on a supposé que y était solution de l'équation différentielle, on a : $\forall x \in \mathbb{R}^+, y(x) = 1 - \lim_\infty(t-x)y'(t) - \int_x^\infty (t-x)p(t)y(t)dt$

Par ailleurs, comme $(t-x)|p(t)y(t)| \leq (t-x)|p(t)|.K$ (où K est une constante), on sait que $t \mapsto (t-x)p(t)y(t)$ est intégrable, et donc que $(t-x).y'(t)$ admet une limite $l \in \mathbb{R}$ en ∞. Si cette limite l était non-nulle, on aurait $y'(t) \sim_\infty \frac{l}{t}$, et alors $\int_0^\infty y'(t)dt = \infty$ (ce qui est absurde, puisque $y(x) = 1 - \int_x^\infty y'(t)dt$).

D'où : $\forall x \in \mathbb{R}^+, y(x) = 1 - \int_0^\infty (t-x)p(t)y(t)dt$

Ce qui termine la phase d'analyse.

On voit donc comment ramener le problème de l'équation différentielle à un problème de point fixe.

Posons donc $E = \{f : [a, \infty[\to \mathbb{R} \ : \text{ continue et bornée}\}$ (on fixera la valeur de a après). On munit de la norme uniforme.

Pour $f \in E$, soit $T(f) : x \geq a \mapsto 1 - \int_0^\infty (t-x)p(t)f(t)dt$

Montrons que E (muni de la norme infini) est complet.

Soit $(f_n)_n \in E^{\mathbb{N}}$ une suite de Cauchy. Pour $\varepsilon > 0$, soit $n_\varepsilon \in \mathbb{N}$ tel que $\forall n, m \geq n_\varepsilon, ||f_n - f_m||_\infty < \varepsilon$. Alors on a aussi, $\forall x \in \mathbb{R}, \forall n, m \geq n_\varepsilon, |f_n(x) - f_m(x)| < \varepsilon$. Donc la suite $(f_n(x))_n$ est de Cauchy, donc converge vers une limite, que l'on note $f(x)$.

Comme $\forall n, m \geq n_\varepsilon, |f_n(x) - f_m(x)| < \varepsilon$, en faisant tendre m vers ∞, on voit que $\forall x \in \mathbb{R}, \forall n \geq n_\varepsilon, |f(x) - f_n(x)| \leq \varepsilon$. D'où $\forall n \geq n_\varepsilon, ||f - f_n||_\infty \leq \varepsilon$. De plus, comme $f = f_n - (f_n - f)$, on sait que $f \in E$ (puisque $f_n \in E$ et que $f_n - f \in E$).

Montrons que T admet un unique point fixe $f \in E$.

Comme E est complet, il suffit de montrer que T est contractante (c'est ici, qu'il faut bien choisir a).

Tout d'abord, il faut montrer que T est à valeurs dans E. Soit $f \in E$, et soit $g = T(f)$. g est clairement continue. De plus, pour $x \geq a$,

$$|g(x)| \leq 1 + ||f||_\infty \int_a^\infty t|p(t)|dt$$

Maintenant, montrons que T est contractante. Soient $f_1, f_2 \in E$ et $g_1 = T(f_1), g_2 = T(f_2)$. On a

$$\forall x \geq a, |g_1(x) - g_2(x)| \leq ||f_1 - f_2||_\infty \int_a^\infty t|p(t)|dt$$

Mais, comme $t \mapsto t|p(t)|$ est intégrable, on sait que $\int_u^\infty t|p(t)|dt \to_\infty 0$. On sait donc qu'il existe $a \geq 0$ tel que $\int_a^\infty t|p(t)|dt < 1$. Pour ce choix de a, T est bien contractante.

Montrons que f est solution de l'équation différentielle sur $[a, \infty[$

Pour $x \geq a, f(x) = 1 - \int_x^\infty tp(t)f(t)dt + x\int_x^\infty p(t)f(t)dt$

Donc f est dérivable sur $[a, \infty[$ et

$$\forall x \geq a, f'(x) = xp(x)f(x) - xp(x)f(x) + \int_x^\infty p(t)f(t)dt = \int_x^\infty p(t)f(t)dt$$

Comme f est bornée, on voit que $\lim \infty f' = 0$, et aussi que f' est dérivable, de dérivée $f''(x) = -p(x)f(x)$.

Par ailleurs, $|f(x) - 1| \leq ||f||_\infty \int_x^\infty t|p(t)|dt$. D'où $\lim_\infty f = 1$.

On sait (d'après la phase d'analyse que f est la seule solution de E sur $[a, \infty[$).

Mais on sait aussi, qu'il existe des solutions de l'équation différentielle définies sur $\mathbb{R}^+$. Parmi elle, on sait qu'il en existe une et une seule qui prolonge f.

2.9 Formule de Stirling

Lemme :

Soit $I_n = \int_0^{\pi/2} (\sin t)^n \, dt$. On a :

- $I_{2n+1} = \frac{2.4\cdots 2n}{1.3\cdots(2n+1)}$
- $I_n \sim \sqrt{\frac{\pi}{2n}}$

preuve :

Montrons que $I_{n+1} = \frac{n}{n+1} I_{n-1}$

En intégrant par parties, on a : $I_{n+1} = \int_0^{\pi/2} (\sin t)(\sin t)^n \, dt = n \int_0^{\pi/2} (\cos t)^2 (\sin t)^{n-1} \, dt$

Donc $I_{n+1} = n \int_0^{\pi/2} \left(1 - (\sin t)^2\right)(\sin t)^{n-1} \, dt = nI_{n-1} - nI_{n+1}$

D'où $I_{n+1} = \frac{n}{n+1} I_{n-1}$

A partir de cette formule, on établit aisément le premier point du lemme.

Montrons que $I_n \sim I_{n+1}$

D'abord $\forall 0 \le t \le \pi/2, 0 \le \sin t \le 1$

donc $\forall 0 \le t \le \pi/2, (\sin t)^{n+1} \le (\sin t)^n$

D'où $I_{n+1} \le I_n$

donc $\frac{I_{n+1}}{I_n} \le 1$

De plus, $\frac{I_{n+1}}{I_n} = \frac{n}{n+1} \frac{I_{n-1}}{I_n} \ge \frac{n}{n+1}$

On a donc $\frac{n}{n+1} \le \frac{I_{n+1}}{I_n} \le 1$

D'où $I_n \sim I_{n+1}$

Montrons que $I_n \sim \sqrt{\frac{\pi}{2n}}$

Comme $\forall n, I_n = \frac{n-1}{n} I_{n-2}$, on sait que la suite $(nI_nI_{n-1})_n$ est constante.

donc $\forall n, nI_nI_{n-1} = \pi/2$

donc $nI_n^2 \sim \pi/2$

d'où $I_n \sim \sqrt{\frac{\pi}{2n}}$

■

Théorème :

$$n! \sim_\infty \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$$

preuve :

Soit $u_n = \frac{n! e^n}{n^{n+1/2}}$, il s'agit de montrer que $(u_n)_n$ converge vers $\sqrt{2\pi}$

Montrons que $(u_n)_n$ **converge vers un nombre** $\lambda > 0$

$\frac{u_{n+1}}{u_n} = (n+1)e\frac{n^{n+1/2}}{(n+1)^{n+1+1/2}} = e\left(\frac{n}{n+1}\right)^{n+1/2} = e\left(1 - \frac{1}{n+1}\right)^{n+1/2}$

donc $\ln u_{n+1} - \ln u_n = 1 + \left(n + \frac{1}{2}\right)\ln\left(1 - \frac{1}{n+1}\right) = 1 - \left(n + \frac{1}{2}\right)\left(\frac{1}{n+1} + \frac{1}{2(n+1)^2} + O\left(\frac{1}{n^3}\right)\right)$

$\ln u_{n+1} - \ln u_n = 1 - \left(\frac{n}{n+1} + \frac{1}{2(n+1)} + \frac{n}{2(n+1)^2} + O\left(\frac{1}{n^2}\right)\right) = \frac{1}{2(n+1)} - \frac{n}{2(n+1)^2} + O\left(\frac{1}{n^2}\right)$

donc $\ln u_{n+1} - \ln u_n = O\left(\frac{1}{n^2}\right)$

donc la série de terme général $(\ln u_{n+1} - \ln u_n)$ est convergeante. Doù, la suite $(\ln u_n)_n$ converge vers un réel l. Finalement, $(u_n)_n$ converge vers $\lambda = e^l > 0$

Montrons que $\lambda = \sqrt{2\pi}$

On sait que $\frac{u_n^2}{u_{2n}} \to \frac{\lambda^2}{\lambda} = \lambda$

D'autre part $\frac{u_n^2}{u_{2n}} = \frac{(n!)^2}{(2n!)} \cdot \frac{(2n)^{2n+1/2}}{n^{2n+1}} = \frac{(n!)^2}{(2n!)} 2^{2n} \sqrt{\frac{2}{n}} = \frac{2.4\cdots 2n}{1.3\cdots(2n-1)} \sqrt{\frac{2}{n}} = (2n+1) I_{2n+1} \sqrt{\frac{2}{n}}$

D'où $\frac{u_n^2}{u_{2n}} \sim 2n \frac{1}{2} \sqrt{\frac{\pi}{n}} \sqrt{\frac{2}{n}} = \sqrt{2\pi}$

■

2.10 Développement asymptotique de $u_{n+1} = u_n - u_n^2$

Références : *[Francinou* et al., *d] p.99*

Lemme :
$\sum_{k=1}^{n} \frac{1}{k} = \ln n + o(\ln n)$

preuve :

la fonction $t \in [1, +\infty[\mapsto \frac{1}{t}$ est décroissante et positive.
On a donc : $\forall k \geq 2, \int_k^{k+1} \frac{dt}{t} \leq \frac{1}{k} \leq \int_{k-1}^{k} \frac{dt}{t}$
D'où $\int_2^{n+1} \frac{dt}{t} \leq \sum_{k=2}^{n} \frac{1}{k} \leq \int_1^n \frac{dt}{t}$
Donc $\ln(n+1) - \ln 2 \leq \sum_{k=2}^{n} \frac{1}{k} \leq \ln n$
Donc $\sum_{k=2}^{n} \frac{1}{k} \sim \ln n$
Donc $\sum_{k=1}^{n} \frac{1}{k} \sim \ln n$
D'où le résultat.

■

Proposition :
Soit $f : [0, b] \longrightarrow \mathbb{R}_+$ où $b > 0$ telle que $f(x) = x - ax^\alpha + o_{x \mapsto 0}(x^\alpha)$ avec $a > 0$ et $\alpha > 1$. Alors, il existe $\eta > 0$ tel que pour toute suite $(u_n)_n$ définie par un $u_0 \in]0, \eta[$ et $u_{n+1} = f(u_n)$, $u_n \sim (a(\alpha-1)n)^{\frac{1}{1-\alpha}}$.

preuve :

Montrons qu'il exite $\eta > 0$ tel que $f([0, \eta[) \subseteq [0, \eta[$
Cela permet de montrer que la suite $(u_n)_n$ est bien définie.
Pour $x \in [0, b]$, on écrit $f(x) = x - ax^\alpha + g(x)$ où $\frac{g(x)}{x^\alpha} \underset{x \to 0}{\longrightarrow} 0$
Alors $f(x) - x = x^\alpha \left(\frac{g(x)}{x^\alpha} - a \right)$
Soit $\eta > 0$ tel que $\forall x \in]0, \eta[, \frac{g(x)}{x^\alpha} - a < 0$
On a donc $\forall x \in]0, \eta[, f(x) - x < 0$
D'où $\forall x \in]0, \eta[, f(x) < x < \eta$
Et par hypothèse, $\forall x \in]0, \eta[, f(x) \geq 0$
D'où le résultat.

Cherchons β tel que $u_{n+1}^\beta - u_n^\beta$ converge
$u_{n+1} = u_n \left(1 - au_n^{\alpha-1} + o\left(u_n^{\alpha-1}\right)\right)$
donc $u_{n+1}^\beta = u_n^\beta \left(1 - a\beta u_n^{\alpha-1} + o\left(u_n^{\alpha-1}\right)\right)$
d'où $u_{n+1}^\beta - u_n^\beta = -a\beta u_n^{\alpha-1+\beta} o\left(u_n^{\alpha-1+\beta}\right)$
on prend donc $\beta = 1 - \alpha < 0$.
on a $u_{n+1}^{1-\alpha} - u_n^{1-\alpha} \longrightarrow a(\alpha - 1)$

Montrons que $u_n \sim (a(\alpha-1)n)^{\frac{1}{1-\alpha}}$

Par le théorème de Césaro, on a : $\frac{1}{n}\sum_{k=0}^{n-1} u_{k+1}^{1-\alpha} - u_k^{1-\alpha} \longrightarrow a(\alpha-1)$

D'où $\frac{1}{n}u_n^{1-\alpha} \to a(\alpha-1)$

Donc $u_n \sim (a(\alpha-1)n)^{\frac{1}{1-\alpha}}$

■

Proposition :

Soit $(u_n)_n$ définie par un $u_0 \in]0,1[$ et $u_{n+1} = u_n - u_n^2$.

Alors $u_n = \frac{1}{n} - \frac{\ln n}{n^2} + o\left(\frac{\ln n}{n^2}\right)$

preuve :

La proposition précédente s'applique ($a = 1$ et $\alpha = 2$).

On a donc : $u_n \sim \frac{1}{n}$

D'autre part : $\frac{1}{u_{n+1}} - \frac{1}{u_n} - 1 = \frac{1-(1-u_n)-u_n(1-u_n)}{u_n(1-u_n)} = \frac{u_n^2}{u_n(1-u_n)} = \frac{1}{1/u_n - 1} \sim \frac{1}{n}$

C'est le terme générale de signe contant d'une série divergente.

On a donc : $\sum_{k=1}^{n-1} \frac{1}{u_{k+1}} - \frac{1}{u_k} - 1 \sim \sum_{k=1}^{n-1} \frac{1}{k}$

D'où $\frac{1}{u_n} - \frac{1}{u_1} - n + 1 = \ln n + o(\ln n)$

Donc $\frac{1}{u_n} = n + \ln n + o(\ln n)$

Donc $u_n = \frac{1}{n+\ln n+o(\ln n)} = \frac{1}{n}\left(1 + \frac{\ln n}{n} + o\left(\frac{\ln n}{n}\right)\right)^{-1} = \frac{1}{n}\left(1 - \frac{\ln n}{n} + o\left(\frac{\ln n}{n}\right)\right)$

Finalement $u_n = \frac{1}{n} - \frac{\ln n}{n^2} + o\left(\frac{\ln n}{n^2}\right)$

■

2.11 Vitesse de convergence des polynômes de Bernstein

Définition :

Pour $f : [0,1] \longrightarrow \mathbb{R}$ continue, on note $w_f(h) = \sup_{|x-y| \leq h} |f(x) - f(y)|$ (où $h \geq 0$)

Proposition :

$\forall f : [0,1] \longrightarrow \mathbb{R}$ continue, $\forall h, \lambda \geq 0, w_f(\lambda h) \leq (\lambda + 1) w_f(h)$

preuve :

Soit $f : [0,1] \longrightarrow \mathbb{R}$

Montrons que w_f est croissante

Soient $0 \leq h_1 \leq h_2$

Alors $\{x, y : |x - y| \leq h_1\} \subseteq \{x, y : |x - y| \leq h_2\}$

D'où $w_f(h_1) \leq w_f(h_2)$

Montrons que $\forall h_1, h_2 \geq 0, w_f(h_1 + h_2) \leq w_f(h_1) + w_f(h_2)$

Soient $h_1, h_2 \geq 0$

Soient x, y tel que $|x - y| \leq h_1 + h_2$

Soit $z = \frac{h_2 x + h_1 y}{h_1 + h_2}$

Alors $|x - z| \leq h_1$ et $|y - z| \leq h_2$

D'où $|f(x) - f(y)| \leq |f(x) - f(z)| + |f(z) - f(y)| \leq w_f(h_1) + w_f(h_2)$

Ceci étant vrai pour tous x, y tels que $|x - y| \leq h_1 + h_2$, on a : $w_f(h_1 + h_2) \leq w_f(h_1) + w_f(h_2)$

On en déduit immédiatement par réccurence que : $\forall n \in \mathbb{N}, \forall h \geq 0, w_f(nh) \leq n w_f(h)$

Montrons que $\forall h, \lambda \geq 0, w_f(\lambda h) \leq (\lambda + 1) w_f(h)$

$w_f(\lambda h) \leq w_f\left(\left(\lfloor \lambda \rfloor + 1\right) h\right) \leq \left(\lfloor \lambda \rfloor + 1\right) w_f(h) \leq (\lambda + 1) w_f(h)$

■

Définition :

Pour $f : [0,1] \longrightarrow \mathbb{R}$, on note $B_n(f)(p) = \mathbb{E}\left[f\left(\frac{X_n^p}{n}\right)\right]$ où $n \in \mathbb{N}^*, p \in [0,1]$ et $(X_n^p)_{n,p}$ sont des variables aléatoires indépendantes, de loi $\mathcal{B}(n,p)$.

Autrement dit : $B_n(f)(p) = \sum_{k=0}^{n} p^k (1-p)^{n-k} f(k/n)$

Proposition :

$\forall f : [0,1] \longrightarrow \mathbb{R}$ continue, $\|B_n(f) - f\|_\infty \leq \frac{3}{2} w_f\left(1/\sqrt{n}\right)$

preuve :

Soit $p \in [0,1]$.

$|B_n(f)(p) - f(p)| = |\mathbb{E}[f(p) - f(X_n^p/n)]| \leq \mathbb{E}[|f(p) - f(X_n^p/n)|] \leq \mathbb{E}[w_f(|p - X_n^p/n|)]$

D'autre part, $w_f(|p - X_n^p/n|) \leq (1 + \sqrt{n}|p - X_n^p/n|) w_f(1/\sqrt{n})$ (d'après la première proposition)

Et $\mathbb{E}[|p - X_n^p/n|] \leq \mathbb{E}\left[(p - X_n^p/n)^2\right]^{1/2} = \mathbb{V}[X_n^p/n]^{1/2} = \frac{1}{n}\mathbb{V}[X_n^p]^{1/2} = \frac{1}{\sqrt{n}}\sqrt{p(1-p)} \leq \frac{1}{2\sqrt{n}}$

La première inégalité ci-dessus est un cas particulier de l'inégalité de Cauchy-Schwarz (ie $\mathbb{E}[|X.Y|] \leq \mathbb{E}[X^2]^{1/2}\mathbb{E}[Y^2]^{1/2}$ avec $Y = 1$)

En combinant les trois inégalités ci-dessus, on obtient :

$$|B_n(f)(p) - f(p)| \leq w_f(1/\sqrt{n})\left(1 + \sqrt{n}\frac{1}{2\sqrt{n}}\right) = \frac{3}{2}w_f\left(1/\sqrt{n}\right)$$

■

2.12 Pobabilité d'extinction du processus de Galton–Watson

Théorème :

Soit Z une variable aléatoire intégrable, à valeurs dans $\mathbb{N}$ telle que $\mathbb{P}(Z=1)<1$. Soit $\left(Z_n^k\right)_{n,k\in\mathbb{N}}$ des variables i.i.d de même loi que Z. On définit une suite de variables aléatoires $(X_n)_n$ récursivement :

$$\begin{cases} X_0 = 1 \\ X_{n+1} = \sum_{k=1}^{X_n} Z_n^k \end{cases}$$

On note $p_e = \mathbb{P}(\exists n. X_n = 0)$ la probabilité d'extinction du processus.

On a alors : $p_e = 1$ ssi $\mathbb{E}[Z] \leq 1$

preuve :

Montrons que $g_{X_{n+1}} = g_{X_n} \circ g_Z$ sur $[0,1]$

On a $\forall t \in [0,1], g_{X_{n+1}}(t) = \mathbb{E}\left[t^{X_{n+1}}\right] = \mathbb{E}\left[\prod_{k=1}^{X_n} t^{Z_n^k}\right] = \mathbb{E}\left[\sum_{x=0}^{\infty} \mathbb{1}_{X_n=x} \prod_{k=1}^{x} t^{Z_n^k}\right] = \sum_{x=0}^{\infty} \mathbb{E}\left[\mathbb{1}_{X_n=x} \prod_{k=1}^{x} t^{Z_n^k}\right]$

Comme X_n est indépendant de Z_n^k (pour tout k), on a :

$\forall t \in [0,1], g_{X_{n+1}}(t) = \sum_{x=0}^{\infty} \mathbb{P}(X_n = x) \prod_{k=1}^{x} \mathbb{E}\left[t^{Z_n^k}\right] = \sum_{x=0}^{\infty} \mathbb{P}(X_n = x) \prod_{k=1}^{x} \mathbb{E}\left[t^{Z}\right] = \sum_{x=0}^{\infty} \mathbb{P}(X_n = x)\, g_Z(t)^x = g_{X_n}(g_Z(t))$

Rq : On en déduit via une récurrence immédiate que $g_{X_n} = g_Z^n$ (ici l'exposant désigne l'itéré pour la loi de composition)

D'où $g_{X_{n+1}} = g_Z \circ g_{X_n}$ (c'est cette relation que l'on utilisera dans la suite)

Montrons que p_e est le plus petit point fixe de g_Z dans $[0,1]$

Par définition, $p_e = \mathbb{P}\left(\bigcup_{n\in\mathbb{N}} \{X_n = 0\}\right) = \lim \mathbb{P}(X_n = 0) = \lim g_{X_n}(0)$ (car $\{X_n = 0\}$ est une suite croissante pour l'inclusion).

On a : $\forall n, g_{X_{n+1}}(0) = g_Z(g_{X_n}(0))$

Comme g_Z est continue sur $[0,1]$ (puisque Z est intégrable), on peut passer à la limite : $p_e = g_Z(p_e)$.

p_e est donc bien point fixe de g_Z.

Soit $p \in [0,1]$ un point fixe de g_Z. Montrons que $p_e \leq p$.

On a $0 \leq p$.

Donc $\forall n, g_{X_n}(0) = g_Z^n(0) \leq g_Z^n(p) = p$ (car g_Z est croissante (c'est une somme de monômes de coefficient positif), et p est un point fixe de g_Z)

rappel : l'exposant dans la relation ci-dessus est l'itération de composition (pas de la multiplication).

En passant à la limite dans l'inégalité ci-dessus, on a : $p_e \leq p$

On a donc bien que p_e est le plus petit point fixe de g_Z dans $[0,1]$.

Montrons que g_Z est convexe sur $[0,1]$, et que, si $\mathbb{P}(Z \geq 2) > 0$ alors g_Z est strictement convexe sur $[0,1]$

$\forall t \in [0,1], g_Z'(t) = \sum_{j=1}^{\infty} \mathbb{P}(Z = j)\, j.t^{j-1}$

Donc g_Z' est croissante sur $[0,1]$, ie g_Z est convexe sur $[0,1]$.

De plus, si $\mathbb{P}(Z \geq 2) > 0$, alors il existe $j \geq 2$, tel que $t \mapsto \mathbb{P}(Z = j)\, j.t^{j-1}$ est strictement croissante sur $[0,1]$. Donc g_Z' est strictement croissante sur $[0,1]$.

Montrons que $\mathbb{E}[Z] \leq 1$ ssi $p_e = 1$

<u>cas 1 :</u> $\mathbb{E}[Z] = g'_Z(1) < 1$

Alors, par convexité de g_Z, on a : $\forall p \in 0,1[, \frac{1-g_Z(p)}{1-p} \leq g'_Z(1) < 1$

D'où $\forall p \in [0,1[, 1 - g_Z(p) < 1 - p$

Donc $\forall p \in [0,1[, p < g_Z(p)$

Donc g_Z n'a aucun point fixe sur $[0,1[$.

Comme 1 est le seul point fixe de g_Z sur $[0,1]$, on a nécessairement $p_e = 1$

<u>cas 2 :</u> $\mathbb{E}[Z] = g'_Z(1) = 1$

Montrons que g_Z est strictement convexe sur [0,1].

On a $1 = \mathbb{E}[Z] = \mathbb{P}(Z = 1) + \sum_n n\mathbb{P}(Z = n)$

Comme par hypothèse, $\mathbb{P}(Z = 1) < 1$, on a $\sum_n n\mathbb{P}(Z = n) > 0$

D'où $\mathbb{P}(Z \geq 2) > 0$, donc g_Z est strictement convexe sur $[0,1]$ (on l'a déjà montré).

Par stricte convextié de g_Z, on a donc $\forall p \in [0,1[, \frac{1-g_Z(p)}{1-p} < g'_Z(1) = 1$

On conclut comme dans le cas 1, que $p_e = 1$.

<u>cas 3 :</u> $\mathbb{E}[Z] = g'_Z(1) > 1$

Soit $h : p \in [0,1] \longmapsto p - g_Z(p)$

Soit $\varepsilon > 0$ tel que $g'_Z(1) > 1 + \varepsilon$. Soit $p_0 \in [0,1[, \frac{1-g_Z(p_0)}{1-p_0} > g'_Z(1) - \varepsilon > 1$

ie $1 - g_Z(p_0) > 1 - p_0$

D'où $h(p_0) > 0$

D'autre part, $h(0) = -g_Z(p_0) \leq 0$.

D'après le théorème des valeurs intermédiaires, il existe $p \in [0, p_0[$ tel que $h(p) = 0$, ie $g_Z(p) = p$.

Donc g_Z admet un point fixe p dans [0,1[. Comme p_e est le plus petit point fixe de g_Z dans $[0,1]$, on a $p_e \leq p < 1$.

D'où $p_e < 1$.

■

2.13 Théorème de Riemann

Références : *[Francinou* et al.*, d] p.217*

Définition :
La série $\left(\sum_{k=0}^{n} a_k\right)_n$ est semi−convergente si la série converge, mais pas absolument.

Théorème (Riemann) :
Soit $\left(\sum_{k=0}^{n} a_k\right)_n$ une série semi−convergente. Alors, pour tout $\alpha \in \mathbb{R}$, il existe $\sigma \in \mathfrak{S}(\mathbb{N})$ tel que $\sum_{n=0}^{\infty} a_{\sigma(n)} = \alpha$

preuve :

Soient $A = \{n \in \mathbb{N} \ : \ a_n \geq 0\}$ et $B = \{n \in \mathbb{N} \ : \ a_n < 0\}$.

Tout d'abord, on sait que A et B sont infinis. En effet, si par exemple, A était fini, alors, en posant $N = 1 + \max A$, on aurait que $\forall n \geq N, a_n < 0$, et alors, la convergence de la série serait équivalente à son absolue convergence (ce qui est faux, puisque la série est semi−convergente).

Définissons $\sigma(n)$ par récurrence sur $n \in \mathbb{N}$:

- $\sigma(0) = 0$
- $\forall n \in \mathbb{N}, \sigma(n+1) = \begin{cases} \min A \backslash \{\sigma(0), \cdots, \sigma(n)\} & \text{si } \sum_{k=0}^{n} a_{\sigma(k)} \leq \alpha \\ \min B \backslash \{\sigma(0), \cdots, \sigma(n)\} & \text{si } \sum_{k=0}^{n} a_{\sigma(k)} > \alpha \end{cases}$

Montrons que σ est une bijection de $\mathbb{N}$ dans $\mathbb{N}$.

Il est évident que σ est injective. En effet, $\forall n \in \mathbb{N}, \forall k < n, \sigma(n) \neq \sigma(k)$ par définition.

Supposons que σ n'est pas surjective. Soit donc $N \in \mathbb{N}$ tel que $N \notin \sigma(\mathbb{N})$. Supposons, par exemple, que $N \in A$. Par construction de σ, on sait alors que $\forall k \in \mathbb{N}$, si $\sigma(k) \in A$, alors $\sigma(k) \leq n$.

On sait donc $\{k \in \mathbb{N} \ : \ \sigma(k) \in A\} \subseteq \sigma^{-1}([\![0, N]\!])$ qui est fini, par injectivité de σ. Soit donc $N = 1 + \max\{k \in \mathbb{N} \ : \ \sigma(k) \in A\}$. On sait alors, que $\forall n \geq N, \sigma(n) \in B$, mais par définition de σ, cela implique que $\forall n \geq N, \sigma(n) = n - N + \sigma(N)$. Cela implique aussi que $\forall n > \sigma(N), n \in B$, et donc par conséquence, que A est fini. Ce qui est absurde.

D'où $\sigma \in \mathfrak{S}_n$.

Montrons que $\sum_{k=0}^{n} a_{\sigma(k)}$ converge vers α.

Comme la série $\sum_n a_n$ converge, on sait que $a_n \to 0$. Cela implique que $a_{\sigma(n)} \to 0$. En effet, Soit $\varepsilon > 0$, soit $n_\varepsilon \in \mathbb{N}$ tel que $\forall n \geq n_\varepsilon, |a_n| < \varepsilon$. Par ailleurs $\{n \in \mathbb{N} : \sigma(n) < n_\varepsilon\} = \sigma^{-1}([\![0, n_\varepsilon - 1]\!])$ qui est fini (puisque σ est injective). Si on pose $N_\varepsilon = 1 + \max\{n \in \mathbb{N} : \sigma(n) < n_\varepsilon\}$, on sait alors que $\forall n \geq N_\varepsilon, |a_{\sigma(n)}| < \varepsilon$.

Soit $\varepsilon > 0$. Soit $N_\varepsilon > 0$ comme précédemment. On sait qu'il existe un $N \in \mathbb{N}$ tel que $\sigma(N) \in A$ et $\sigma(N+1) \in B$ (on a déjà vu que les $\sigma(n)$ ne pouvait pas tous rester dans A ni dans B).

Soit $S_n = \sum_{k=0}^{n} a_{\sigma(k)}$. Il suffit maintenant de montrer que $\forall n \geq N, |S_n - \alpha| \leq \varepsilon$.

Comme $\sigma(N) \in A, \sigma(N+1) \in B$, on sait que $S_{N-1} \leq \alpha$ et $S_N > \alpha$ (par définition de σ). On sait donc que $|S_N - \alpha| \leq |S_N - S_{N-1}| = |u_{\sigma(N)}| \leq \varepsilon$. Autrement dit, $S_N \in [\alpha - \varepsilon, \alpha + \varepsilon]$.

Soit $n > N$. Supposons que $|S_n - \alpha| > \varepsilon$. Par exemple, supposons que $S_n > \alpha + \varepsilon$. On a alors $S_{n-1} = S_n - a_{\sigma(n)} > \alpha$. Mais alors, par définition de σ, on sait que $a_{\sigma(n)} < 0$, et alors $S_n < S_{n-1}$. En réitérant le raisonnement, on obtient :

$$\alpha + \varepsilon < S_n < S_{n-1} < S_{n-2} < \cdots < S_N$$

En particulier, $|S_N - \alpha| > \varepsilon + \alpha$ ce qui est absurde (on l'a déjà montré).

Donc, finalement, $\forall n \geq N, |S_n - \alpha| \leq \varepsilon$

■

2.14 Convergence de l'algorithme LR

2.15 Intégrale de Dirichlet

Références : *[Francinou* et al., *f]* p.214

Il s'agit de montrer que $\int_0^{+\infty} \frac{\sin t}{t} dt = \frac{\pi}{2}$

Soit $F : x \mapsto \int_0^{+\infty} e^{-xt} \frac{\sin t}{t} dt$

Montrons que F est définie sur $\mathbb{R}_+$

Soit $f : (x,t) \in \mathbb{R}_+ \times \mathbb{R}_+^* \mapsto e^{-xt} \frac{\sin t}{t}$.

Pour tout $x > 0$, $t \mapsto f(x,t)$ est intégrable sur $\mathbb{R}_+$ car elle se prolonge par continuité en 0, et $f(x,t) = O_{t\infty}\left(\frac{1}{t^2}\right)$.

Donc F est définie sur $\mathbb{R}_+^*$. Montrons que F est définie en 0.

La fonction $t \mapsto \frac{\sin t}{t}$ est intégrable en 0 (par continuité), mais pas en $+\infty$. Il suffit donc de vérifier que $\int_1^{+\infty} \frac{\sin t}{t} dt$ est définie et finie.

Pour $X \geq 1$, on a : ${}_1^X \frac{\sin t}{t} dt = \left[\frac{-\cos t}{t}\right]_1^X - \int_1^X \frac{\cos t}{t^2} dt$

D'où, en faisant tendre X vers $+\infty$:

$$\int_1^{+\infty} \frac{\sin t}{t} dt = \cos 1 - \int_1^{+\infty} \frac{\cos t}{t^2} dt < +\infty$$

puisque $\frac{\cos t}{t^2} = O_{t\to\infty}\left(\frac{1}{t^2}\right)$

Montrons que F est $\mathcal{C}^1$ sur $\mathbb{R}_+^*$

Pour cela, on va montrer que F est $\mathcal{C}^1$ sur $]a, +\infty[$ pour tout $a > 0$.

Soit donc $a > 0$.

La fonction f est $\mathcal{C}^1$ sur $(\mathbb{R}_+^*)^2$.

On a $\forall (x,t) \in (\mathbb{R}_+^*)^2$, $\frac{\partial f}{\partial x}(x,t) = -e^{-xt} \sin t$

De plus, $\forall x \geq a, \forall t > 0, \left|\frac{\partial f}{\partial x}(x,t)\right| \leq e^{-at}$ qui est intégrable sur $\mathbb{R}_+$

Par le théorème du caractère $\mathcal{C}^1$ sous le signe intégral, on a bien, que F est $\mathcal{C}^1$ sur $]a, +[$.

Comme cela est vrai pour tout $a > 0$, on a bien que F est $\mathcal{C}^1$ sur $\mathbb{R}_+^*$.

On sait même que :

$$\forall x > 0, F'(x) = \int_0^{+\infty} e^{-xt} \sin t dt = -Im\left(\int_0^{+\infty} e^{-(x-i)t} dt\right) = Im\left(\frac{1}{i-x}\right) = -\frac{1}{1+x^2}$$

On sait donc qu'il existe $C \in \mathbb{R}$ telle que $\forall x > 0, F(x) = C - \arctan x$

Comme $|F(x)| \leq \int_0^{+\infty} e^{-xt} dt = \frac{1}{x} \underset{x\to+\infty}{\longrightarrow} 0$, on sait que $C = \frac{\pi}{2}$.

D'où $\forall x > 0, F(x) = \frac{\pi}{2} - \arctan x$

Montrons que F est continue en 0

On aura alors démontré que $\int_0^{+\infty} \frac{\sin t}{t} dt = F(0) = \frac{\pi}{2}$

On écrit : $\forall x \geq 0, F(x) = F_1(x) + F_2(x)$ où $F_1(x) = \int_0^1 e^{-xt} \frac{\sin t}{t} dt$ et $F_2(x) = \int_1^{+\infty} e^{-xt} \frac{\sin t}{t} dt$

F_1 est $\mathcal{C}^1$ sur $\mathbb{R}_+$, car on a la domination $\left|\frac{\partial f}{\partial x}(x,t)\right| \leq 1$ qui est intégrable sur $[0,1]$.

Il reste à démontrer que F_2 est continue en 0. Pour cela, on va montrer que $G : x \in \mathbb{R} \mapsto \int_1^{+\infty} \frac{e^{-(x-i)t}}{t} dt$ est continue en 0, puisque F_2 est la partie imaginaire de G.

Pour $X \geq 1$, on a :

$$\int_1^X \frac{e^{-(x-i)t}}{t} dt = \left[\frac{e^{-(x-i)t}}{(i-x)t}\right]_1^X + \frac{1}{i-x}\int_1^X \frac{e^{-(x-i)t}}{t^2} dt$$

Comme $\left|\frac{e^{-(x-i)t}}{t^2}\right| \leq \frac{1}{t^2}$, on sait que $t \mapsto \frac{e^{-(x-i)t}}{t^2}$ est intégrable sur $[1, +\infty[$. On a donc :

$$\forall x \geq 0, G(x) = \frac{e^{i-x)}}{x-i} + \frac{1}{i-x}\int_1^{+\infty} \frac{e^{-(x-i)t}}{t^2} dt$$

Et la fonction $x \mapsto \int_1^{+\infty} \frac{e^{-(x-i)t}}{t^2} dt$ est continue sur $\mathbb{R}_+$, car $(x,t) \mapsto \frac{e^{-(x-i)t}}{t^2}$ est continue sur $\mathbb{R}_+ \times [1, +\infty[$ et on a la domination $\left|\frac{e^{-(x-i)t}}{t^2}\right| \leq \frac{1}{t^2}$. On en déduit que G est continue sur $\mathbb{R}_+$, donc F_2 aussi, et F aussi.

2.16 Théorème d'inversion de Fourier

Définition :

Soit $f \in \mathbb{L}^1(\mathbb{R})$, on définit sa transformée de Fourier $\widehat{f} : x \in \mathbb{R} \mapsto \int_{\mathbb{R}} f(t)e^{i.x.t}dt$

Lemme :

Pour toutes fonctions $f, g \in \mathbb{L}^1(\mathbb{R})$ telles que $f * g \in \mathbb{L}^1(\mathbb{R})$, on a : $\widehat{f * g} = \widehat{f}.\widehat{g}$

Définition :

Pour $\sigma > 0$, on définit la fonction gaussienne $g_\sigma : t \in \mathbb{R} \mapsto \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{x^2}{2\sigma^2}}$

Lemme :

Pour toute fonction $f \in \mathbb{L}^1(\mathbb{R})$, $f * g_\sigma$ converge vers f dans $\mathbb{L}^1$ quand σ tend vers 0.

Lemme :

Soit $(f_n)_n$ une suite de fonctions $\mathbb{L}^1(\mathbb{R})$, et $f \in \mathbb{L}^1(\mathbb{R})$. Si f_n converge vers f dans $\mathbb{L}^1(\mathbb{R})$, alors il existe une sous-suite $(f_{\varphi(n)})_n$ qui converge vers f presque partout.

Théorème :

Soit $f \in \mathbb{L}^1(\mathbb{R})$ telle que $\widehat{f} \in \mathbb{L}^1(\mathbb{R})$.

On a : p.p.$x \in \mathbb{R}, \widehat{\widehat{f}}(-x) = 2\pi f(x)$

preuve :

On va d'abord prouver le théorème dans le cas où $f = g_\sigma$ pour un $\sigma > 0$ quelconque

Montrons que $\forall x \in \mathbb{R}, \widehat{g_\sigma}(x) = e^{-\frac{x^2\sigma^2}{2}}$

$\widehat{g_\sigma}(x) = \frac{1}{\sigma\sqrt{2\pi}} \int_{\mathbb{R}} e^{-\frac{t^2}{2\sigma^2}+i.x.t}dt$

$\widehat{g_\sigma}'(x) = \frac{i}{\sigma\sqrt{2\pi}} \int_{\mathbb{R}} t.e^{-\frac{t^2}{2\sigma^2}+i.x.t}dt$ (cf théorème de dérivation sous l'intégrale)

Par ailleurs, $\frac{1}{\sigma\sqrt{2\pi}} \int_{\mathbb{R}} \left(-\frac{t}{\sigma^2} + i.x\right) e^{-\frac{t^2}{2\sigma^2}+i.x.t}dt = 0$

D'où $\frac{i}{\sigma^2}\widehat{g_\sigma}'(x) + i.x.\widehat{g_\sigma}(x) = 0$

Donc $\widehat{g_\sigma}' + \sigma^2.x.\widehat{g_\sigma} = 0$

On sait donc que $\forall x \in \mathbb{R}, \widehat{g_\sigma}(x) = \widehat{g_\sigma}(0).e^{-\frac{x^2\sigma^2}{2}} = e^{-\frac{x^2\sigma^2}{2}}$

On a donc : $\widehat{g_\sigma} = \frac{\sqrt{2\pi}}{\sigma} g_{1/\sigma}$

D'où $\widehat{\widehat{g_\sigma}} = \frac{\sqrt{2\pi}}{\sigma}\widehat{g_{1/\sigma}} = \frac{\sqrt{2\pi}}{\sigma}\sigma\sqrt{2\pi}g_\sigma$

On a donc bien : $\widehat{\widehat{g_\sigma}} = 2\pi g_\sigma$

On va maintenant prouver le cas général du théorème

Soit $f \in \mathbb{L}^1(\mathbb{R})$ telle que $\widehat{f} \in \mathbb{L}^1(\mathbb{R})$.

D'après les lemmes, il existe une suite $(\sigma_n)_n \in (\mathbb{R}_+^*)^{\mathbb{N}}$ qui converge vers 0, telle que $(f * g_{\sigma_n})_n$ converge vers f dans $\mathbb{L}^1(\mathbb{R})$.

Soit $x \in \mathbb{R}$.

Montrons que $\widehat{\widehat{f * g_{\sigma_n}}}(-x) \to 2\pi f(x)$

$\widehat{\widehat{f * g_{\sigma_n}}}(-x) = \int_{\mathbb{R}} \widehat{f * g_{\sigma_n}}(t) e^{-i.x.t} dt = \int_{\mathbb{R}} \widehat{f}(t)\widehat{g_{\sigma_n}}(t) e^{-i.x.t} dt = \int_{\mathbb{R}} \int_{\mathbb{R}} f(u) e^{i.t(u-x)} \widehat{g_{\sigma_n}}(t) du\ dt$

Par le théorème de Fubini-Lebesgue, on a donc :

$\widehat{\widehat{f * g_{\sigma_n}}}(-x) = \int_{\mathbb{R}} \int_{\mathbb{R}} f(u) e^{i.t(u-x)} \widehat{g_{\sigma_n}}(t) dt\ du = \int_{\mathbb{R}} f(u) \widehat{\widehat{g_{\sigma_n}}}(u-x) du$

Comme $\widehat{\widehat{g_\sigma}} = 2\pi g_\sigma$, on a :

$\widehat{\widehat{f * g_{\sigma_n}}}(-x) = 2\pi \int_{\mathbb{R}} f(u) g_{\sigma_n}(u-x) = 2\pi \int_{\mathbb{R}} f(u) g_{\sigma_n}(x-u) = 2\pi f * g_{\sigma_n}(x) \to 2\pi f(x)$

Montrons que $\widehat{\widehat{f * g_{\sigma_n}}}(-x) \to \widehat{\widehat{f}}(-x)$

En reprenant le début du calcul précédent, et en utilisant le fait que $\forall x \in \mathbb{R}, g_\sigma(x) = e^{-\frac{x^2\sigma^2}{2}}$, on a :

$\widehat{\widehat{f * g_{\sigma_n}}}(-x) = \int_{\mathbb{R}} \widehat{f}(t)\widehat{g_{\sigma_n}}(t) e^{-i.x.t} dt = \int_r \widehat{f}(t) e^{-i.x.t} e^{-\frac{x^2\sigma^2}{2}} dt$

En utilisant le théorème de convergence dominée (ce qui est possible car $\widehat{f} \in \mathbb{L}^1(\mathbb{R})$), on a :

$\widehat{\widehat{f * g_{\sigma_n}}}(-x) \to \widehat{\widehat{f}}(-x)$

■

2.17 Comportement au bord du disque de convergence

Références *: [Gourdon,] p.246*

2.18 Formule Sommatoire de Poisson

Références *: [Gourdon,] p.272*

2.19 Calcul de sommes de séries

Références *: [Francinou* et al.*, e] p.288*

3 Développements Informatique

3.1 Hauteur moyenne d'un abre binaire de recherche (ABR)

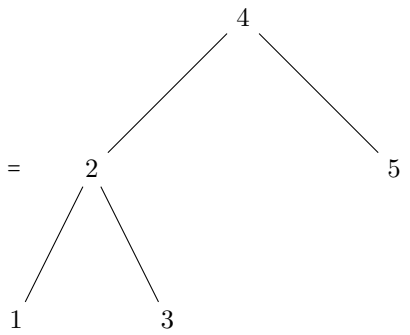
Références : *[Cormen* et al., *] p.279*

Remarque : la preuve du Cormen est incomplète et en partie fausse.

Définition :
Pour $\sigma \in \mathfrak{S}_n$, on définit A_n^σ l'ABR initialement vide, obtenu après insertions de $\sigma(1)$, puis $\sigma(2)$,$\cdots$, puis $\sigma(n)$.

exemple : $n = 5$ et σ : $\begin{cases} 1 & \mapsto & 4 \\ 2 & \mapsto & 2 \\ 3 & \mapsto & 1 \\ 4 & \mapsto & 3 \\ 5 & \mapsto & 5 \end{cases}$

$A_n^\sigma =$



Lemme :
Si σ une variable aléatoire de loi $\mathcal{U}(\mathfrak{S}_n)$, alors $\sigma(1)$ suit la loi $\mathcal{U}(\llbracket 1, n \rrbracket)$

preuve :

Soit $1 \leq k \leq n$.

On a : $\mathbb{P}(\sigma(1) = k) = \frac{|\{\tau \in \mathfrak{S}_n : \tau(1) = k\}|}{n!} = \frac{(n-1)!}{n!} = \frac{1}{n}$

L'avant dernière égalité vient du fait que, le nombre de permutations de $\llbracket 1, n \rrbracket$, qui envoie 1 sur k, est exactement le nombre de bijections de $\llbracket 2, n \rrbracket$ dans $\llbracket 1, n \rrbracket \backslash \{k\}$ (ie le nombre de permutations d'un ensemble à $n-1$ éléments). ■

Théorème :
Soit σ une variable aléatoire de loi $\mathcal{U}(\mathfrak{S}_n)$. On a :

$$\mathbb{E}[h(A_n^\sigma)] \leq 3 \log_2(n+3)$$

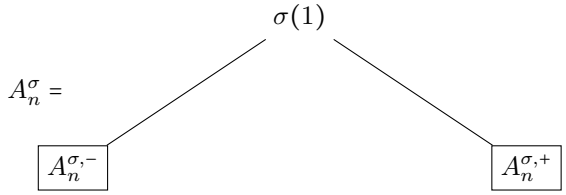
preuve :

Soit $Y_n = 2^{h(A_n^\sigma)}$

Montrons que $\mathbb{E}[Y_n] \leq \binom{n+3}{3}$ (par récurrence sur n)

On sait que $Y_0 = 1 = \binom{0+3}{3}$. Il suffit donc de montrer l'hérédité. On suppose donc que $\forall k \in [\![0, n-1]\!], \mathbb{E}[Y_k] \leq \binom{k+3}{3}$

On sait que A_n^σ est de la forme :



Soit K le nombre de nœuds de $A_n^{\sigma,-}$. On a $K = |\{1 \leq i \leq n : \sigma(i) < \sigma(1)\}| = \sigma(1) - 1$.

Donc, d'après le Lemme, K suit la loi $\mathcal{U}([\![0, n-1]\!])$

Pour $0 \leq k \leq n-1$, introduisons τ_k une variable aléatoire de loi $\mathcal{U}(\mathfrak{S}_k)$ telle que, conditionnellement à $\{K = k\}$, $A_n^{\sigma,-} = A_k^{\tau_k}$

Soit $0 \leq k \leq n-1$ fixé. Soient $a_1 < a_2 < \cdots < a_k$ tels que $\{\sigma(a_1), \cdots, \sigma(a_k)\} = [\![1, k]\!]$ (les a_i sont donc des variables aléatoires). On définit $\forall i \in [\![1, n]\!], \tau_k(i) = \sigma(a_i)$

Par définition de τ_k, on a que $A_n^{\sigma,-} = A_k^{\tau_k}$ conditionnellement à $\{K = k\}$.

Soit $\nu \in \mathfrak{S}_k$, Montrons que $\mathbb{P}(\tau_k = \nu) = \frac{1}{k!}$

Pour cela, il suffit de calculer le nombre de $\sigma \in \mathfrak{S}_n$ telles que $\tau_k = \nu$ ie $\forall i \in [\![1, k]\!], \sigma(a_i) = \nu(i)$. Ce sont les σ de la forme :

$$\sigma : \begin{cases} \cdots & a_1 & \cdots & a_2 & \cdots & \cdots & \cdots & a_k & \cdots \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \cdots & \nu(1) & \cdots & \nu(2) & \cdots & \cdots & \cdots & \nu(k) & \cdots \end{cases}$$

Il y en a donc : $\binom{n}{k}(n-k)!$. En effet, il faut choisir les positions des a_i $(1 \leq i \leq k)$ (d'où le $\binom{n}{k}$), puis les images des a_i par σ sont imposées ainsi que leur ordre, mais on peut permuter les $n-k$ autres éléments (d'où le $(n-k)!$).

On a donc : $\mathbb{P}(\tau_k = \nu) = \frac{\binom{n}{k}(n-k)!}{n!} = \frac{1}{k!}$

Finalement, on a bien : $A_n^{\sigma,-} = A_k^{\tau_k}$ conditionnellement à $\{K = k\}$, et τ_k suit la loi $\mathcal{U}(\mathfrak{S}_k)$.

De même, on a : $A_n^{\sigma,+} = A_{n-k-1}^{\nu_{n-k-1}}$ conditionnellement à $\{K = k\}$, et ν_{n-k-1} suit la loi $\mathcal{U}(\mathfrak{S}_{n-k-1})$.

Revenons au calcul de $\mathbb{E}[Y_n]$.

On sait (par définition de la hauteur) que : conditionnellement à $\{K = k\}$, $Y_n = 2\max(Y_k, Y_{n-k-1})$.

D'où :

$$\begin{aligned} \mathbb{E}[Y_n] &= \sum_{k=0}^{n-1} \mathbb{P}(K = k) . \mathbb{E}[Y_n | K = k] \\ &= \frac{2}{n} \sum_{k=0}^{n-1} \mathbb{E}[\max(Y_k, Y_{n-k-1})] \\ &\leq \frac{2}{n} \sum_{k=0}^{n-1} \mathbb{E}[Y_k + Y_{n-k-1}] \qquad (\forall a, b \geq 0, \max(a, b) \leq a + b) \end{aligned}$$

$$\leq \frac{4}{n}\sum_{k=0}^{n-1}\mathbb{E}[Y_k] \qquad \left(\sum_{k=0}^{n-1} Y_{n-k-1} = \sum_{k=0}^{n-1} Y_k\right)$$

$$\leq \frac{4}{n}\sum_{k=0}^{n-1}\binom{k+3}{3} \qquad \text{(hypothèse de récurrence)}$$

$$\leq \frac{4}{n}\sum_{k=0}^{n-1}\binom{k+4}{4} - \binom{k+3}{4} \qquad \text{(formule du triangle de Pascal)}$$

$$\leq \frac{4}{n}\binom{n+3}{4} = \frac{4}{n}\frac{(n+3)(n+2)(n+1)n}{4.3.2.1} = \binom{n+3}{3}$$

On a donc bien montré que : $\forall n \in \mathbb{N}, \mathbb{E}[Y_n] \leq \binom{n+3}{3}$

Montrons maintenant que $\mathbb{E}[h(A_n^\sigma)] \leq 3\log_2(n+3)$

On a : $\mathbb{E}[Y_n] \leq \binom{n+3}{3} \leq (n+3)^3$

Par le lemme de Jensen, on a :

$$2^{\mathbb{E}[h(A_n^\sigma)]} \leq \mathbb{E}\left[2^{h(A_n^\sigma)}\right] = \mathbb{E}[Y_n] \leq (n+3)^3$$

$$\mathbb{E}[h(A_n^\sigma)] \leq 3\log_2(n+3)$$

■

Conséquence : Le tri par insertion sur les ABR a une complexité moyenne $O(n.\log n)$ (on a même la majoration explicite $3n\log_2(n+3)$). Ceci est la borne optimale de complexité pour les tris par comparaisons (même pour les complexités en moyenne).

3.2 Classe universelle de fonctions de hachage

Références *: [Cormen* et al., *] p.248*

3.3 Transformée de Fourier rapide

Références *: [Cormen* et al., *] p.830*

3.4 Circuit additionneur à n bits

Références *: [Albert* et al., *] p.368-374*

3.5 Tri bitonique

3.6 Algorithme CYK

3.7 Algorithme Floyd–Warshall

Références *: [Cormen* et al.*,] p.639*

3.8 Automate de recherche de motifs

Références *: [Cormen* et al., *] p.915*

3.9 Codage de Huffman

Références *: [Cormen* et al., *] p.399*

3.10 Algorithme de MacNaughton & Yamada

Références *: [Albert* et al., *] p.285*

3.11 La fonction d'Ackermann n'est pas récursive primitive

Références : *[Corges,] p.126-131*

Définition :

pour $n, m \in \mathbb{N}$, on définit :

$$\begin{cases} a(0,n) = n+1 \\ a(m+1,0) = a(1,m) \\ a(m+1,n+1) = a(m,a(m+1,n)) \end{cases}$$

Lemme :

On a les propriétés suivantes :

(1) $\forall n, a(2,n) \geq 2n$

(2) $\forall m,n, a(m,n) > m+n$

(3) $\forall m,n, a(m,n+1) > a(m,n)$

(4) $\forall m,n, a(m+1,n) \geq a(m,n+1)$

(5) $\forall m,n, a(m+1,n) > a(m,n)$

(6) $\forall m_1,m_2, \exists m, \forall n, a(m_1,a(m_2,n)) \leq a(m,n)$

(7) $\forall r \in \mathbb{N}^*, \forall m_1,\cdots,m_r, \exists m, \forall n \sum_{i=1}^{r} a(m_i,n) \leq a(m,n)$

(8) $\forall f : \mathbb{N}^k \longrightarrow \mathbb{N}$ récursive primitive, $\exists m, \forall (n_1,\cdots,n_k), f(n_1,\cdots,n_k) \leq a\left(m, \sum_{i=1}^{k} n_i\right)$

preuve :

(1) :

Montrons que $\forall n, a(1,n) = n+2$ **(par récurrence sur** n**)**

$a(1,0) = a(0,1) = 2$

Si $a(1,n) = n+2$, alors $a(1,n+1) = a(0,a(1,n)) = 1 + a(1,n) = n+3$

Montrons que $\forall n, a(2,n) = 2n+3$ **(par récurrence sur** n**)**

$a(2,0) = a(1,1) = 3$

Si $a(2,n) = 2n+3$ alors $a(2,n+1) = a(1,a(2,n)) = 2 + a(2,n) = 2n+5$

(2) :

Montrons le résultat par récurrence sur m.

$\forall n, a(0,n) = n+1 > n$

Soit $m \in \mathbb{N}$ **fixé. Supposons que** $\forall n, a(m,n) \geq m+n+1$ **et montrons que** $\forall n, a(m+1,n) \geq m+n+2$

On fait une récurrence sur n.

$a(m+1,0) = a(m,1) \geq m+2$

Soit n fixé, supposons que $a(m+1,n) \geq m+n+2$, montrons que $a(m+1,n+1) \geq m+n+3$

$a(m+1,n+1) = a(m,a(m+1,n)) \geq m+1+a(m+1,n)$ (cf première hypothèse de récurrence)

$a(m+1,n+1) \geq m+1+m+n+2 = 2m+n+3 \geq m+n+3$ (cf seconde hypothèse de récurrence)

(3) :

Soient $n, m \in \mathbb{N}$ fixés. Montrons que $a(m,n) < a(m,n+1)$

cas 1 : Si $m = 0$, alors $a(0,n+1) = n+2 > n+1 = a(0,n)$

cas 2 : Si $m > 0$, alors $a(m,n+1) = a(m-1,a(m,n)) > m-1+a(m,n)$ (cf (2))

donc $a(m,n+1) > a(m,n)$

(4) :

Soient $n, m \in \mathbb{N}$ fixés. Montrons que $a(m+1,n) \geq a(m,n+1)$

cas 1 : Si $n = 0$, alors $a(m+1,0) = a(m,1)$

cas 2 : Si $n > 0$, alors $a(m+1,n) = a(m,a(m+1,n-1)) \geq a(m,m+n+1)$ (cf (3))

donc $a(m+1,n) \geq a(m,n+1)$

(5) :

$\forall m,n, a(m+1,n) \geq a(m,n+1) > a(m,n)$ (cf (3) et (4))

(6) :

Soit $m_0 = \max(m_1,m_2)$.

On a : $\forall n, a(m_1,a(m_2,n)) \leq a(m_0,a(m_0,n)) \leq a(m_0,a(m_0+1,n)) = a(m_0+1,n+1) \leq a(m_0+2,n)$

(7) : Montrons le résultat par récurrence sur r

$r = 1$ **:** il n'y a rien à montrer

$r = 2$ **:** soit $m_0 = \max(m_1,m_2)$.

On a donc $\forall n, a(m_1,n) + a(m_2,n) \leq 2a(m_0,n) \leq a(2,a(m_0,n))$ (cf (1))

Soit m tel que $\forall n, a(2,a(m_0,n)) \leq a(m,n)$ (cf (6))

On a donc $\forall n, a(m_1,n) + a(m_2,n) \leq a(m,n)$

hérédité :

Soient $m_1, \cdots, m_{r+1}$ des entiers ($r \geq 2$).

Soit m' tel que $\forall n, \sum_{i=1}^{r} a(m_i,n) \leq a(m',n)$ (cf hypothèse de récurrence)

Soit m tel que $\forall n, a(m',n) + a(m_{r+1},n) \leq a(m,n)$ (cf cas $r = 2$)

On a donc : $\forall n, \sum_{i=1}^{r+1} a(m_i,n) \leq a(m,n)$

(8) :

Montrons le résultat par récurrence sur f.

Zero : $f : (n_1, \cdots, n_k) \in \mathbb{N}^k \mapsto 0$

alors $\forall (n_1, \cdots, n_k), f(n_1, \cdots, n_k) = 0 \leq a\left(0, \sum_{i=1}^{k} n_i\right)$

Projection : $f : (n_1, \cdots, n_k) \in \mathbb{N}^k \mapsto n_i$

alors $\forall (n_1, \cdots, n_k), f(n_1, \cdots, n_k) = n_i \leq a\left(0, \sum_{j=1}^{k} n_j\right)$

Successeur : $f : n \in \mathbb{N} \mapsto n+1$

alors $\forall n, f(n) = n+1 = a(0,n)$

Composition : $f : (n_1, \cdots, n_k) \in \mathbb{N}^k \mapsto h(g_1(n_1, \cdots, n_k), \cdots, g_p(n_1, \cdots, n_k))$

Soit m' tel que $\forall (n_1, \cdots, n_p), h(n_1, \cdots, n_p) \leq a\left(m', \sum_{j=1}^{p} n_j\right)$

pour $1 \leq j \leq k$, soit m_j tel que $\forall (n_1, \cdots, n_k), g_j(n_1, \cdots, n_k) \leq a\left(m_j, \sum_{i=1}^{k} n_i\right)$

Soit m'' tel que $\forall n, \sum_{j=1}^{p} a(m_j, n) \leq a(m'', n)$

Soit m tel que $\forall n, a(m', a(m'', n)) \leq a(m, n)$.

Donc $\forall (n_1, \cdots, n_k), f(n_1, \cdots, n_k) \leq a\left(m, \sum_{i=1}^{k} n_i\right)$

Récurrence :

$$\begin{cases} \mathrm{f}(\mathrm{n}_1, \cdots, n_k, 0) & = & \mathrm{g}(\mathrm{n}_1, \cdots, n_k) \\ \mathrm{f}(\mathrm{n}_1, \cdots, n_k, x+1) & = & \mathrm{h}(\mathrm{n}_1, \cdots, n_k, x, f(n_1, \cdots, n_k, x)) \end{cases}$$

Soit m' tel que $\forall (n_1, \cdots, n_k), g(n_1, \cdots, n_k) \leq a\left(m', \sum_{i=1}^{k} n_i\right)$

Soit m'' tel que $\forall (n_1, \cdots, n_k), \forall x, y, h(n_1, \cdots, n_k, x, y) \leq a\left(m'', x + y + \sum_{i=1}^{k} n_i\right)$

Soit m_0 tel que $\forall n, a(m'', a(2, n)) \leq a(m_0, n)$.

Soit $m = \max(m', m_0 + 1)$.

Soit $(n_1, \cdots, n_k,)$ fixé.

Montrons que $\forall x, f(n_1, \cdots, n_k, x) \leq a\left(m, \sum_{i=1}^{k} n_i\right)$ (par récurrence sur x)

$f(n_1, \cdots, n_k, 0) = g(n_1, \cdots, n_k) \leq a\left(m', \sum_{i=1}^{k} n_i\right) \leq a\left(m, \sum_{i=1}^{k} n_i\right)$

Soit x un entier, supposons que $f(n_1, \cdots, n_k, x) \leq a\left(m, \sum_{i=1}^{k} n_i\right)$.

Alors $f(n_1, \cdots, n_k, x+1) = h(n_1, \cdots, n_k, x, f(n_1, \cdots, n_k, x)) \leq a\left(m'', x + \sum_{i=1}^{k} n_i + f(n_1, \cdots, n_k, x)\right)$

$f(n_1, \cdots, n_k, x+1) \leq a\left(m'', x + \sum_{i=1}^{k} n_i + a\left(m, x + \sum_{i=1}^{k} n_i\right)\right) \leq a\left(m'', 2a\left(m, x + \sum_{i=1}^{k} n_i\right)\right)$

$f(n_1, \cdots, n_k, x+1) \leq a\left(m'', a\left(2, a\left(m, x + \sum_{i=1}^{k} n_i\right)\right)\right) \leq a\left(m - 1, a\left(m, x + \sum_{i=1}^{k} n_i\right)\right)$

$f(n_1, \cdots, n_k, x+1) \leq a\left(m, x + 1 + \sum_{i=1}^{k} n_i\right)$

■

Théorème :

La fonction d'Ackermann n'est pas récursive primitive.

preuve :

Supposons que la fonction a est récursive primitive. Alors, la fonction $f : n \in \mathbb{N} \mapsto a(n, n)$ est aussi récursive primitive. Soit donc $m \in \mathbb{N}$ tel que $\forall n, f(n) \leq a(m, n)$ (cf (8)).

On a alors : $a(m+1, m+1) = f(m+1) \leq a(m, m+1) < a(m+1, m+1)$

Ce qui est absurde, d'où le résultat.

■

3.12 Toute fonction Turing–calculable est récursive

Références *: [Carton,] p.185*

3.13 Théorème de Savitch

Références *: [Carton,] p.219*

3.14 Décidabilité de l'arithmétique de Presburger

Références : *[Dowek,] p.174-177*

On considère le langage $\mathcal{L}$ constitué des constantes 0 et 1, des symboles de fonction binaire + et −, d'un symbole de prédicat binaire $\leq$ et, pour chaque $n \in \mathbb{N}$, d'un symbole de prédicat unaire $Mult_n$.

Définition :

On appelle le modèle $\mathbb{Z}$, l'ensemble $\mathbb{Z}$ qui interprète naturellement $0, 1, +, -, \leq$, et qui interprète $Mult_n(x)$ comme "x est un multiple de n".

Proposition :

Pour toute proposition A sans quantificateur dans $\mathcal{L}$, il existe une proposition B sans quantificateur, telle que la proposition $(\exists x.A) \Leftrightarrow B$ est valide dans le modèle $\mathbb{Z}$.

preuve :

Soit A une proposition sans quantificateur de $\mathcal{L}$.

On va d'abord construire une proposition A' sans quantificateur telle que :

$$\begin{cases} (i) \exists x.A \Leftrightarrow \exists x'.A' \text{ est valide dans le modèle } \mathbb{Z} \\ (ii) A' \text{ ne contient pas de négation, et les propositions atomiques sont de la forme } x' \leq t, t \leq x', \\ \quad u \leq t, Mult_n(x'+t), Mult_n(t) \text{ où } t, u \text{ sont des termes ne contenant ni } x \text{ ni } x' \end{cases}$$

On va construire A' à partir de A via des transformations successives. On illustrera les différentes transformation sur l'exemple $A = (1 \leq 3.x) \wedge \neg(7 - x \leq x - 1)$

Soit A_0 obtenue à partir de A en supprimant les négations, via les transformations suivantes :

- $\neg\top \rightsquigarrow \bot \quad , \quad \neg\bot \rightsquigarrow \top$
- $\neg(C \wedge D) \rightsquigarrow (\neg C) \vee (\neg D) \quad , \quad \neg(C \vee D) \rightsquigarrow (\neg C) \wedge (\neg D) \quad , \quad \neg\neg C \rightsquigarrow C$
- $\neg(t \leq u) \rightsquigarrow u + 1 \leq t$
- $\neg(Mult_n(t)) \rightsquigarrow Mult_n(t+1) \vee \cdots \vee Mult_n(t+n-1)$

Sur l'exemple $A_0 = (1 \leq 3.x) \wedge (x \leq 7 - x)$

Soit A_1 obtenue à partir A_0 en mettant, pour chaque inéquation, les x du même côté de l'inéquation (de telle sorte que le coefficient devant le x soit positif), et le reste de l'autre côté.

Sur l'exemple $A_1 = (1 \leq 3.x) \wedge (2.x \leq 7)$

Soit A_2 obtenu à partir de A_1 en remplaCcant chaque inéquation $u \leq t$ par $k.u \leq k.t$ où $k \in \mathbb{N}^*$ (chaque inéquation a un k différent a priori) et chaque $Mult_n(t)$ par $Mult_{k.n}(k.t)$ où $k \in \mathbb{N}^*$ (encore une fois, a priori, les k ne sont pas les mêmes) de manière a obtenir le même coefficient s pour x dans toutes les propositions atomiques.

Sur l'exemple $A_2 = (2 \leq 6.x) \wedge (6.x \leq 21)$

Soit A' obtenue à partir de A_2 en remplaCcant tous les $s.x$ par x' et en ajoutant la proposition atomique $Mult_s(x')$.

Sur l'exemple $A' = (2 \leq x') \wedge (x' \leq 21) \wedge Mult_6(x')$

Il est clair que $\exists x.A \Leftrightarrow \exists x'.A'$ est valide dans le modèle $\mathbb{Z}$.

On va construire une proposition B sans quantificateur telle que $(\exists x'.A') \Leftrightarrow B$ est valide dans le modèle $\mathbb{Z}$

Soit r un multiple commun de tous les entiers n tels que la proposition atomique $Mult_n(x'+t)$ apparaisse dans A'.

Soit E l'ensemble des termes t tels que la proposition atomique $x' \leq t$ apparaisse dans A'. Soit A'' la proposition obtenue à partir de A' en remplaCcant les propositions atomiques de la forme $x' \leq t$ par $\perp$ et $t \leq x'$ par $\top$.

Soit B la disjonction des propositions de la forme :

- $(i/x')\, A''$ où $i \in [\![0, r-1]\!]$ (1)
- $((t-j)/x')\, A'$ où $t \in E, j \in [\![0, r-1]\!]$ (2)

Soit $y1, \cdots y_n$ les variables de A' distinctes de x'. On écrira $A'[p, q_1, \cdots, q_n] = (p/x', q_1/y_1, \cdots, q_n/y_n)A'$, $A''[p, q_1, \cdots, q_n] = (p/x', q_1/y_1, \cdots, q_n/y_n)A''$ et $B[q_1, \cdots, q_n] = (q_1/y_1, \cdots, q_n/y_n)B$.

Rq : par construction, A' et A'' sont équivalentes pour des valeurs de x' "grandes", et A'' est périodique en la valeur de x' de période r. En effet, quand x' devient arbitrairement grand, les propositions $x' \leq t$ deviennent fausses, les $t \leq x'$ deviennent vraies, et les $Mult_n(x'+t)$ deviennent périodiques de période r.

Il nous reste donc à montrer que, pour tout $q_1, \cdots, q_n \in \mathbb{Z}$, il existe $p \in \mathbb{Z}$ tel que $A'[p, q_1, \cdots, q_n]$ soit valide si et seulement si $B[q_1, \cdots, q_n]$ soit valide.

Soient $q_1, \cdots, q_n \in \mathbb{Z}$ fixés.

Supposons qu'il existe $p \in \mathbb{Z}$ tel que $A'[p, q_1, \cdots, q_n]$ soit valide

cas 1 : $\forall v \in \mathbb{Z}, A'[p + v.r, q_1, \cdots, q_n]$ est valide.

On peut alors prendre $p' \in \mathbb{Z}$ suffisament grand tel que $A'[p', q_1, \cdots, q_n]$ soit valide et tel que $A'[p', q_1, \cdots, q_n]$ est équivalente à $A''[p', q_1, \cdots, q_n]$. Donc $A''[p', q_1, \cdots, q_n]$ est valide, mais comme A'' est périodique en la valeur de x', on sait qu'il existe un $p'' \in [\![0, r-1]\!]$ tel que $A[p'', q_1, \cdots, q_n]$ est valide. Donc $B[q_1, \cdots, q_n]$ est valide (car une proposition de la forme (1) est valide).

cas 2 : $\exists p' \in \mathbb{Z}$ tel que $A'[p', q_1, \cdots, q_n]$ est valide mais $A'[p'+r, q_1, \cdots, q_n]$ n'est pas valide.

Or, les seules propositions atomiques de A' qui peuvent changer de valeurs de vrai à faux entre $x' = p'$ et $x' = p' + r$ sont celles de la forme $x' \leq t$ (on rappelle qu'il n'y a pas de négation dans A', donc si A' passe de vrai à faux, c'est nécessairement, qu'une des propositions passe de vrai à faux). On sait donc qu'il existe un $t \in E$ tel que $p' \leq t[q_1, \cdots, q_n]$ et $t[q_1, \cdots, q_n] < p' + r$. Donc $\exists j \in [\![0, r-1]\!], p' = t[q_1, \cdots, q_n] - j$. Donc $B[q_1, \cdots, q_n]$ est valide (car une proposition de la forme (2) est valide).

Réciproquement, supposons que $B[q_1, \cdots, q_n]$ est valide

cas 1 : Il existe $i \in [\![0, r-1]\!]$ tel que $A''[i, q_1, \cdots, q_n]$ est valide.

Comme A'' est périodique en x' de période r, on peut trouver un p arbitrairement grand tel que $A''[i, q_1, \cdots, q_n]$ est équivalente à $A''[p, q_1, \cdots, q_n]$, qui est elle-même équivalente à $A'[p, q_1, \cdots, q_n]$. On a donc bien trouvé un $p \in \mathbb{Z}$ tel que $A'[p, q_1, \cdots, q_n]$ est valide.

cas 2 : Il existe $j \in [\![0, r-1]\!]$ tel que $A'[t[q_1, \cdots, q_n] - j, q_1, \cdots, q_n]$ est valide.

Il existe donc bien un $p = t[q_1, \cdots, q_n] - j \in \mathbb{Z}$ tel que $A'[p, q_1, \cdots, q_n]$ est valide.

■

Proposition :

Pour toute proposition A de $\mathcal{L}$, il existe une proposition B sans quantificateurs telle que $A \Leftrightarrow B$ est valide dans le modèle $\mathbb{Z}$.

preuve :

On remplace les propositions de la forme $\forall x.C$ par $\neg\exists x.\neg C$, puis on élimine les quantificateurs en procédant par récurrence, en utilisant la proposition précédente. ■

Théorème :

L'ensemble des propositions de $\mathcal{L}$ valide dans le modèle $\mathbb{Z}$ est décidable.

preuve :

La proposition précédente permet de se ramener au cas des propositions closes et sans quantificateur, qui est un cas décidable.

■

Théorème (Presburger) :

L'ensemble des propositions formées dans le langage $0, S, +, =$ et valide dans le modèle $\mathbb{N}$ est décidable.

preuve :

On va construire une fonction qui associe à chaque proposition A du langage $0, S, +, =$ une proposition $|A|$ du langage $0, 1, +, -, \leq$ telle que A est valide dans le modéle $\mathbb{N}$ si et seulement si $|A|$ est valide dans le modèle $\mathbb{Z}$. Cette fonction permet de ramener la question de la décidabilité des propositions de l'arithmétique de Presburger à la question de décidabilité des propositions de $0, 1, +, -, \leq$ dans le modèle $\mathbb{Z}$, dont on a prouvé qu'elles étaient décidables.

- $|0| = 0$, $|x| = x$, $|S(t)| = t + 1$, $|t + u| = |t| + |u|$
- $|t = u| = (|t| \leq |u|) \wedge (|u| \leq |t|)$
- $|\top| = \top$, $|\bot| = \bot$, $|\neg A| = \neg|A|$, $|A \wedge B| = |A| \wedge |B|$, $|A \vee B| = |A| \vee |B|$
- $|\forall x.A| = \forall x(0 \leq x \Rightarrow |A|)$, $|\exists x.A| = \exists x(0 \leq x \wedge |A|)$

■

3.15 Indécidabilité de la terminaison des sytèmes de réécriture

Références *: [Baader et Nipkow,] p.94*

3.16 Le problème de la couverture de sommets est NP–complet

Références : *[Carton,] p.210-212*

Définition :

Soit $G = (S, A)$ un graphe non orienté.

On dit que $\mathcal{C} \subseteq S$ est une couverture de G si $\forall \{u, v\} \in A, u \in \mathcal{C}$ ou $v \in \mathcal{C}$.

Si on note k le cardinal de $\mathcal{C}$, on dit que $\mathcal{C}$ est une k–couverture de G.

On considère la problème $Couv$: $\begin{cases} \text{Données : G graphe (non orienté), k entier} \\ \text{Question : Existe-t-il une k-couverture ?} \end{cases}$

Il est clair que $Couv$ est NP. Montrons que ce problème est NP–difficile.

On va réduire le problème $3-SAT$: $\begin{cases} \text{Données : } \varphi = \bigwedge_{i=1}^{r} l_1^i \vee l_2^i \vee l_3^i \text{ où les } l_j^i \text{ sont des littéraux.} \\ \text{Question : } \varphi \text{ est satisfaisable ?} \end{cases}$

Soit donc $\varphi = \bigwedge_{i=1}^{r} l_1^i \vee l_2^i \vee l_3^i$ une instance de $3-SAT$. Soit X l'ensemble des variables de φ. Soit $\overline{X} = \{\overline{x} : x \in X\}$.

Soit $n = |X|$.

Soit $S = X \cup \overline{X} \cup \left\{l_j^i : 1 \leq i \leq r, 1 \leq j \leq 3\right\}$

Soit $A = A_1 \cup A_2 \cup A_3$ avec $A_1 = \{\{x, \overline{x}\} : x \in X\}$ et $A_2 = \bigcup_{i=1}^{r} \left\{\{l_{j_1}^i, l_{j_2}^i\} : 1 \leq j_1, j_2 \leq 3, j_1 \neq j_2\right\}$

et $A_3 = \{\{l, l_j^i\} : l \in X \cup \overline{X}, 1 \leq i \leq r, 1 \leq j \leq 3, l$ et l_j^i correspondent au même litéral$\}$

Soit $G = (S, A)$ et $k = 2r + n$, une instance de $Couv$

Montrons que φ est satisfaisable ssi G possède une $2r+n$–couverture.

Rq : toute couverture de G est de taille au moins $2r + n$. En effet, la couverture doit contenir au moins x ou $\overline{x}$ pour chaque $x \in X$ pour recouvrir A_1, et la couverture doit contenir au moins deux sommets de $\{l_1^i, l_2^i, l_3^i\}$ pour chaque i, pour recouvrir le "triangle".

Supposons que φ a un modèle $\nu : X \to \{0, 1\}$

Pour chaque $1 \leq i \leq r$, soit $1 \leq j_i \leq 3$ tel que $\nu(l_{j_i}^i) = 1$

Soit $\mathcal{C} = \left\{l \in X \cup \overline{X} : \nu(l) = 1\right\} \cup \bigcup_{i=1}^{r} \{l_j^i : j \neq j_i\}$

On a $|\mathcal{C}| = n + 2r$. Il suffit donc de montrer que $\mathcal{C}$ est une couverture de G.

Soit $a \in A$. On considère trois cas.

cas 1 : $a = \{x, \overline{x}\} \in A_1$. Alors $x \in \mathcal{C}$ ou $\overline{x} \in \mathcal{C}$ puisque $\nu(x) = 1$ ou $\nu(\overline{x}) = 1$

cas 2 : $a \in A_2$. Comme dans chaque "triangle" de A_2, il y a exactement deux sommets dans $\mathcal{C}$, on sait que les arêtes du triangles sont forcément toutes couvertes par $\mathcal{C}$.

cas 3 : $a = \{l, l_j^i\} \in A_3$. Il y a deux possibilités : soit $\nu(l) = 1$, alors $l \in \mathcal{C}$, soit $\nu(l) = 0$, mais alors $j \neq j_i$ et donc $l_j^i \in \mathcal{C}$.

$\mathcal{C}$ est bien une $2r + n$–couverture de G.

Supposons que $\mathcal{C}$ soit une $2r+n$–couverture de G

On a : $2r + n = |\mathcal{C}| = |\mathcal{C} \cap (X \cup \overline{X})| + |\mathcal{C} \cap \bigcup_{i=1}^{r} \{l_1^i, l_2^i, l_3^i\}|$

Comme $\mathcal{C}$ recouvre A_1, on a $|\mathcal{C} \cap (X \cup \overline{X})| \geq n$, et comme $\mathcal{C}$ recouvre A_2, on a $|\mathcal{C} \cap \bigcup_{i=1}^{r} \{l_1^i, l_2^i, l_3^i\}| \geq 2r$

En combinant ces inégalités avec l'égalité au-dessus, on obtient $|\mathcal{C} \cap (X \cup \overline{X})| = n$ et $|\mathcal{C} \cap \bigcup_{i=1}^{r} \{l_1^i, l_2^i, l_3^i\}| = 2r$.

On peut alors définir $\nu : X \to \{0,1\}$ tel que $\nu(l) = 1$ ssi $l \in \mathcal{C}$ (pour $l \in X \cup \overline{X}$)

Montrons que ν est un modèle de φ.

Soit $1 \leq i \leq r$ fixé. Avec le même type de raisonnement que précédemment on montre que $|C \cap \{l_1^i, l_2^i, l_3^i\}| = 2$. Soit $1 \leq j \leq 3$ tel que $l_j^i \notin \mathcal{C}$, et soit $l \in X \cup \overline{X}$ tel que l et l_j^i correspondent au même litéral. Comme $\mathcal{C}$ recouvre $\{l, l_j^i\}$, et que $l_j^i \notin \mathcal{C}$, on sait que $l \in \mathcal{C}$, ie $\nu(l) = 1$.

On vient donc de montrer que $\forall 1 \leq i \leq r, \exists 1 \leq j \leq 3, \nu(l_j^i) = 1$, c'est-à-dire ν est bien un modèle de φ.

3.17 Complétude de la résolution

3.18 Elimination des coupures en calcul des séquents

Références *: [Dowek,] p.156*

3.19 Correction d'un algorithme d'unification

Références *: [Baader et Nipkow,] p.73*

3.20 Lemme de Newmann

Références *: [Baader et Nipkow,] p.29*

3.21 Correction de Dijkstra

Algorithme 1 : l'algorihme de Dijkstra

Entrées : $G = (S, A)$ graphe orienté,$w : A \to \mathbb{R}_+$,$s_0 \in S$

pour $s \in S$ **faire**
  $\delta(s) \leftarrow \infty$
fin
$\delta(s_0) \leftarrow 0$
$F \leftarrow S$
tant que $F \neq \varnothing$ **faire**
  $s \leftarrow \arg\min_{s' \in F} \delta(s')$
  $F \leftarrow F \backslash \{s\}$
  pour $s' \in S$ *tel que* $(s, s') \in A$ **faire**
    $\delta(s') \leftarrow \min(\delta(s'), \delta(s) + w(s, s'))$
  fin
  $(*)$
fin
retourner δ

On va montrer la correction de l'algorithme en prouvant deux invariants au niveau de $(*)$ dans l'algorithme :

$I1 : \forall u \in S, \delta(u) < \infty \Rightarrow \delta(u)$ est la longueur d'un chemin de s_0 à u

$$I2 : \begin{cases} \text{(i) :} & \forall u \in S \backslash F, \delta(u) = d(s_0, u) \\ \text{(ii) :} & \forall u \in F, \text{ s'il existe } s_0 \to \cdots \to v \to u \text{ un plus court chemin tel que } v \in S \backslash F, \text{ alors } \delta(u) = d(s_0, u) \end{cases}$$

La correction partielle de l'algorithme vient de la condition de sortie de boucle et de la propriété $I2, (i)$. De plus, la terminaison de l'algortithme étant évidente ($|F|$ décrémente à chaque itération), on obtient la correction totale.

Dans la preuve des invariants, si x est une variable, on notera $\underline{x}$ la valeur de x à l'itération précédente, et $\overline{x}$ sa valeur à l'itération actuelle.

Preuve de l'invariant $I1$

Au premier tour de boucle, si $\delta(u) < \infty$, alors $u = s_0$ ou $(s_0, u) \in A$. Dans le premier cas, on a $\delta(u) = 0 = d(s_0, u)$, et dans le second $\delta(u) = w(s_0, u)$ (ce qui est bien la longueur d'un chemin de s_0 à u).

Supposons que $\forall u \in S, \delta(u) < \infty \Rightarrow \underline{\delta}(u)$ est la longueur d'un chemin de s_0 à u

Montrons que cela reste vrai à l'itération actuelle.

Soit $u \in S$ tel que $\overline{\delta}(u) < \infty$.

cas 1 : $\overline{\delta}(u) = \underline{\delta}(u)$. Il n'y a rien à montrer.

cas 2 : $\overline{\delta}(u) = \underline{\delta}(\overline{s}) + w(\overline{s}, u)$ et $(\overline{s}, u) \in A$. Par hypothèse $\underline{\delta}(\overline{s})$ est la longueur d'un chemin de s_0 à $\overline{s}$ et donc $\underline{\delta}(\overline{s}) + w(\overline{s}, u)$ est la longueur d'un chemin de s_0 à u.

Preuve de l'invariant $I2$

Montrons le résultat au premier tour de boucle.

(i) : $S \backslash F = \{s_0\}$, et $\delta(s_0) = 0 = d(s_0, s_0)$

(ii) : Soit $u \in F = S \backslash \{s_0\}$ tel qu'il existe un plus court chemin de s_0 à u dont le prédecesseur de u est s_0. Dans

ce cas, on peut se ramener à un pus court chemin de de la forme $s_0 \to u$ (quitte à court-circuiter le chemin). Par définition de l'algorithme, on a $\delta(u) \leq \delta(s_0) + w(s_0, u) = w(s_0, u) = d(s_0, u)$. Par ailleurs, comme $\delta(u) \geq d(s_0, u)$, on a bien $\delta(u) = d(s_0, u)$.

Supposons que $\underline{(i)}$ et $\underline{(ii)}$ sont vraies (ie les propriétés portent sur les variables soulignées), et montrons que $\overline{(i)}$ et $\overline{(ii)}$ sont vraies.

(i) :

Soit $u \in S \backslash \overline{F}$.

cas 1 : $u \in S \backslash \underline{F}$. Alors $\overline{\delta}(u) \leq \underline{\delta}(u)$ (par définition de l'algorithme)

et $\underline{\delta}(u) = d(s_0, u)$ par $\underline{(i)}$.

Par ailleurs, on sait que $d(s_0, u) \leq \overline{\delta}(u)$ (cf $I1$)

D'où $d(s_0, u) \leq \overline{\delta}(u) \leq \underline{\delta}(u) = d(s_0, u)$

Donc $\overline{\delta}(u) = d(s_0, u)$

cas 2 : $u = \overline{s}$. Démontrons que $\overline{\delta}(u) = d(s_0, u)$ par l'absurde. Supposons donc que $\overline{\delta}(u) > d(s_0, u)$.

Soit $s_0 = v_0 \to v_1 \to \cdots v_k = u$ un plus court chemin de s_0 à $u = \overline{s}$. $s_0 = v_0 \in S \backslash \underline{F}$ et $u = v_k \in \underline{F}$. Soit donc j tel que $v_j \in S \backslash \underline{F}$ et $v_{j+1} \in \underline{F}$.

On sait alors que $d(s_0, v_{j+1}) \leq d(s_0, u)$ et que $s_0 = v_0 \to v_1 \to \cdots v_{j+1}$ est un plus court chemin de s_0 à v_{j+1}. Donc par $\underline{(ii)}$, on a que $\underline{\delta}(v_{j+1}) = d(s_0, v_{j+1})$.

D'où $\underline{\delta}(v_{j+1}) = d(s_0, v_{j+1}) \leq d(s_0, u) < \overline{\delta}(u)$

Donc $\underline{\delta}(v_{j+1}) < \underline{\delta}(\overline{s})$.

Mais $v_{j+1} \in \underline{F}$. L'inégalité stricte précédente est donc en contradiction avec la définition de la variable s de l'algorithme.

(ii) :

Soit $u \in \overline{F}$ tel qu'il existe un plus court chemin de s_0 à u de la forme $s_0 \to \cdots \to v \to u$ avec $v \in S \backslash \overline{F}$.

cas 1 : $v \in S \backslash \underline{F}$

Alors $d(s_0, u) \leq \overline{\delta}(u) \leq \underline{\delta}(u) = d(s_0, u)$ (cf $\underline{(ii)}$)

Donc $\overline{\delta}(u) = d(s_0, u)$

cas 2 : $v = \overline{s}$

Alors $\overline{\delta}(u) \leq \underline{\delta}(\overline{s}) + w(\overline{s}, u) = d(s_0, \overline{s}) + w(\overline{s}, u)$ (cf $\overline{(i)}$)

D'où $d(s_0, u) \leq \overline{\delta}(u) \leq d(s_0, v) + w(v, u) = d(s_0, u)$

Donc $\overline{\delta}(u) = d(s_0, u)$

3.22 Algorithme d'approximation pour le problème de la couverture d'ensembles

Références *: [Cormen* et al.*,] p.1029*

Considérons le problème de la couverture d'ensembles :

$$\begin{cases} \text{Entrées :} & \text{un ensemble } X, \text{ une famille } \mathcal{F} \text{ de parties de } X \\ \text{Sortie :} & \text{une partie minimale } \mathcal{C} \subseteq \mathcal{F} \text{ telle que } X = \bigcup_{S \in \mathcal{C}} S \end{cases}$$

Le problème de décision associé est NP–complet. En effet on peut réduire le problème de couverture de sommets : Si $G = (S, A)$ est un graphe (non-orienté), on pose $X = A$ et $\mathcal{F} = \{\{a : \ s \text{ est une extrémité de } a\} : s \in S\}$. Bien que ce problème est NP–complet, il existe un algorithme d'approximation.

Algorithme 2 : algorithme d'approximation du problème de couverture d'ensembles

Entrées : X un ensemble, $\mathcal{F}$ un ensemble de parties de X

$U \leftarrow X$

$\mathcal{C} \leftarrow \varnothing$

tant que $U \neq \varnothing$ **faire**

  choisir $S \in \mathcal{F}$ qui maximise $|S \cap U|$

  $U \leftarrow U \backslash S$

  $\mathcal{C} \leftarrow \mathcal{C} \cup \{S\}$

fin

retourner $\mathcal{C}$

Lemme :

Soit $H(n) = \sum_{k=1}^{n} \frac{1}{k}$.

On a : $H(n) \leq \ln n + 1$

Théorème :

L'algorithme précédent est un algorithme d'approximation à temps polynomial, avec garantie de performance en $(\ln|X| + 1)$.

preuve :

Il est clair que l'algorithme s'éxécute en temps polynomial.

Notons k le nombre d'itérations de l'algorithme. Soit $\mathcal{C}$ la couverture renvoyée par l'algorithme et $\mathcal{C}^*$ une couverture optimale.

Notons $S_0, S_1, \cdots, S_{k-1}$ les éléments de $\mathcal{F}$ choisies successivement par l'algorithme.

La couverture de que renvoit l'algorithme est donc de taille k, chaque $S_i \in \mathcal{C}$ a un poids de 1. L'idée de la preuve est de répartir uniformément le poids de chaque S_i sur l'ensemble des éléments recouverts pour la première fois par S_i.

Pour $x \in X$, on note $0 \leq i \leq k$ minimale tel que $x \in S_i$, et on pose :

$$c_x = \frac{1}{|S_i(S_0 \cup \cdots \cup S_{i-1})|}$$

D'après les notations, on a :

$$\sum_{x\in X} c_x = \sum_{i=0}^{k-1} \sum_{x\in S_i\setminus(S_0\cup\cdots\cup S_{i-1})} c_x = \sum_{i=0}^{k-1} 1 = k = |\mathcal{C}|$$

Donc : $|\mathcal{C}| = \sum_{x\in X} c_x$

Par ailleurs, comme chaque $x \in X$ appartient à au moins un élément de $\mathcal{C}^*$, on a :

$$\sum_{S\in\mathcal{C}^*} \sum_{x\in S} c_x \geq \sum_{x\in X} c_x$$

D'où :

$$|\mathcal{C}| \leq \sum_{S\in\mathcal{C}^*} \sum_{x\in S} c_x \qquad (*)$$

Montrons maintenant

$$\forall S \in \mathcal{F}, \sum_{x\in S} c_x \leq H(|S|) \qquad (**)$$

Une fois que l'on aura démontré $(**)$, alors, en utilisant $(*)$ et le lemme, on aura :

$$|\mathcal{C}| \leq \sum_{S\in\mathcal{C}^*} H(|S|) \leq |\mathcal{C}^*|.H\left(\max\{|S| : S \in \mathcal{F}\}\right) \leq |\mathcal{C}^*|.H(|X|) \leq |\mathcal{C}^*|.(\ln|X| + 1)$$

Il ne reste qu'à montrer l'inégalité $(**)$.

Soit $S \in \mathcal{F}$. Pour $0 \leq i \leq k$, notons $u_i = |S\setminus(S_0 \cup \cdots \cup S_i)|$ le nombre d'éléments qui ne sont pas couverts à l'issue de la i^{eme} étape de l'algorithme. On note, de plus, $u_{-1} = |S|$.

Soit l l'indice minimal tel que $u_l = 0$. On sait que $u_{i-1} \geq u_i$ et qu'il y a exactement $u_{i-1} - u_i$ éléments recouverts pour la première fois par S_i $(0 \leq i \leq l)$. D'où :

$$\sum_{x\in S} c_x = \sum_{i=0}^{l} (u_{i-1} - u_i) \frac{1}{|S_i\setminus(S_0 \cup \cdots \cup S_{i-1})|}$$

D'autre part, comme S_i est un choix glouton de l'algorithme, on a :

$$|S_i\setminus(S_0 \cup \cdots \cup S_{i-1})| \geq |S\setminus(S_0 \cup \cdots \cup S_{i-1})| = u_{i-1}$$

On a donc :

$$\begin{aligned}
\sum_{x\in S} c_x &\leq \sum_{i=1}^{k} (u_{i-1} - u_i) \frac{1}{u_{i-1}} \\
&= \sum_{i=1}^{k} \sum_{j=u_i+1}^{u_{i-1}} \frac{1}{u_{i-1}} \\
&\leq \sum_{i=0}^{l} \sum_{j=u_i+1}^{u_{i-1}} \frac{1}{j} \\
&= \sum_{i=0}^{l} \left(\sum_{j=1}^{u_{i-1}} \frac{1}{j} - \sum_{j=1}^{u_i} \frac{1}{j} \right)
\end{aligned}$$

$$= \sum_{i=0}^{k} (H(u_{i-1}) - H(u_i))$$

$$= H(u_{-1}) - H(u_l)$$

$$= H(|S|)$$

On a bien montré l'inégalité $(**)$.

■

4 Références

[Albert *et al.*,] Albert, L., Gastin, P., Petazzoni, B., Petit, A., Puech, N. et Weil, P. *Cours et exercices d'informatique. Classes préparatoires,* 1^{er} *et* 2^{nd} *cycles universitaires.* Vuibert.

[Baader et Nipkow,] Baader, F. et Nipkow, T. *Term rewriting and all that.* Cambridge University Press.

[Carton,] Carton, O. *Langages formels. Calculabilité et complexité.* Vuibert.

[Choquet,] Choquet, G. *Cours de topologie.* Dunod.

[Corges,] Corges, C. *Machines de Turing et automates cellulaires.* ellipses.

[Cormen *et al.*,] Cormen, T., Leiserson, C., Rivest, R. et Stein, C. *Introduction à l'algorithmique.* Dunod.

[Dowek,] Dowek, G. *Les démonstrations et les algorithmes. Introduction à la logique et à la calculabilité.* Les éditions de l'École Polytechnique.

[Francinou *et al.*, a] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, algèbre 1.* Cassini.

[Francinou *et al.*, b] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, algèbre 2.* Cassini.

[Francinou *et al.*, c] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, algèbre 3.* Cassini.

[Francinou *et al.*, d] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, analyse 1.* Cassini.

[Francinou *et al.*, e] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, analyse 2.* Cassini.

[Francinou *et al.*, f] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, analyse 3.* Cassini.

[Francinou *et al.*, g] Francinou, S., Gianella, H. et Nicolas, S. *exercices de mathématiques, oraux X-ENS, analyse 4.* Cassini.

[Gourdon,] Gourdon, X. *les maths en tête. Analyse.* ellipses.

[Mansuy et Mneimné,] Mansuy, R. et Mneimné, R. *Algèbre linéaire. Réduction des endomorphismes.* Vuibert.

[Perrin,] Perrin, D. *Cours d'algèbre.* ellipses.

[Rouvière,] Rouvière, F. *petit guide de calcul différentiel.* Cassini.