Agrégation de Mathématiques
Option Informatique

Maxime Bombar
bombar@crans.org

1er mai 2021

TABLE DES MATIÈRES

TODO LIST

Première partie

Couplage

CHAPITRE 1

ALGÈBRE

101	Groupe opérant sur un ensemble. Exemples et applications.	25, 12
104	Groupes finis. Exemples et applications.	12, 29
105	Groupes des permutations d'un ensemble fini. Applications	12, 09
106	Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.	17, 14
108	Exemples de parties génératrices d'un groupe. Applications.	24, 09
120	Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.	29, 18
121	Nombres premiers. Applications.	28, 18
123	Corps finis. Applications.	02, 25
126	Exemples d'équations en arithmétique.	28, 25
141	Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.	02, 18
151	Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.	33, 10
152	Déterminant. Exemples et applications.	30, 09
153	Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie.	10, 07
156	Exponentielle de matrices. Applications.	04, 06
157	Endomorphismes trigonalisables. Endomorphismes nilpotents.	07, 17
159	Formes linéaires et dualité en dimension finie. Exemples et applications.	10, 33
162	Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.	19, 09
170	Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.	25, 06
182	Applications des nombres complexes à la géométrie	30, 24
183	Utilisation des groupes en géométrie.	12, 24
190	Méthodes combinatoires, problèmes de dénombrement.	25, 01

CHAPITRE 2

ANALYSE

203	Utilisation de la notion de compacité.	08, 14
208	Espaces vectoriels normés, applications linéaires continues. Exemples.	08, 14, 27
214	Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.	33, 04
219	Extremums : Existence, caractérisation, recherche. Exemples et applications.	33, 20
220	Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2.	16, 27
221	Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.	16, 27
223	Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.	32 /!\ , 05
224	Exemples de développements asymptotiques de suites et de fonctions	05, 15
226	Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.	05, 19
228	Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.	15, 27
229	Fonctions monotones. Fonctions convexes. Exemples et applications.	20, 03
230	Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.	31, 22, 23
233	Analyse numérique matricielle : résolution approchée de systèmes linéaire, recherche de vecteurs propres, exemples.	13, 19
236	Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables	11, 15
239	Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.	15, 03, 11
243	Convergence des séries entières, propriétés de la somme. Exemples et applications.	01, 31
246	Séries de Fourier. Exemples et applications.	22, 23
250	Transformation de Fourier. Applications.	11, 22
260	Espérance, variance et moments d'une variable aléatoire.	26, 23
264	Variables aléatoires discrètes. Exemples et applications.	26, 23
265	Exemples d'études et d'applications de fonctions usuelles et spéciales.	03

CHAPITRE 3

INFO

901	Structures de données. Exemples et applications.	07, 11
903	Exemples d'algorithmes de tri. Correction et complexité.	19, 22
907	Algorithmique du texte. Exemples et applications.	03, 09
909	Langages rationnels et Automates finis. Exemples et applications.	03, 18
912	Fonctions récursives primitives et non primitives. Exemples.	02, 16, ??
913	Machines de TURING. Applications.	16, 12
914	Décidabilité et indécidabilité. Exemples.	18, 10
915	Classes de complexité. Exemples.	01, 12
916	Formules du calcul propositionnel : Représentation, formes normales, satisfiabilité. Applications.	20, 01
918	Systèmes formels de preuve en logique du premier ordre. Exemples.	17, 14
921	Algorithmes de recherche et structures de données associées.	07, 11
923	Analyse lexicale et syntaxique. Applications.	05, 10
924	Théories et modèles en logique du premier ordre. Exemples.	17, 18
925	Graphes : représentation et algorithmes.	01, 15
926	Analyse des algorithmmes : complexité. Exemples	07, 19, 11
927	Exemples de preuve d'algorithme : Correction, terminaison.	15, 13
928	Problèmes NP-Complets : Exemples et réductions.	08, 04
929	Lambda-Calcul pur comme modèle de calcul. Exemples.	??, ??
930	Sémantique des langages de programmation. Exemples.	21, 13
931	Schémas algorithmiques. Exemples et applications.	04, 09
932	Fondement théorique des bases de données relationnelles.	06, 08

Deuxième partie

Développements

CHAPITRE 4

MATHS

01 Nombres de Bell

01.1 Références :

— *Algèbre 1*, FGN [FN07a]

— *40 développements d'Analyse*, J et L Bernis [Ber18]

01.2 Développement

Pour tout $n \geq 1$ on note B_n le nombre de partitions de $\{1, \dots, n\}$. On pose de plus $B_0 := 1$. Alors

$$B_n := \frac{1}{e} \sum_{p=0}^{\infty} \frac{p^n}{p!}$$

01.3 Preuve

Démonstration. Soient $n \in \mathbb{N}$ et $\mathcal{P}_{n+1}$ l'ensemble des partitions de $\{1, \dots, n+1\}$. Pour dénombrer $\mathcal{P}_{n+1}$ on classe les partitions selon le cardinal de l'ensemble qui contient $n+1$

Soit $\mathcal{P}_{n+1,k}$ l'ensemble des partitions de $\{1, \dots, n+1\}$ tel que le paquet contenant $n+1$ contient k autres éléments.

Insérer un dessin ici, ça sera plus clair !

Ainsi,

$$\mathcal{P}_{n+1} = \bigsqcup_{k=0}^{n} \mathcal{P}_{n+1,k}$$

Dénombrement de $\mathcal{P}_{n+1,k}$: Le paquet contenant $n+1$ est formé d'un choix de k autres éléments dans $\{1, \dots, n\}$. Il y a $\binom{n}{k}$ tels choix. La réunion des autres paquets forme

une partition d'un ensemble à $n+1-(k+1) = n-k$ éléments. Or le nombre de partitions ne dépend que du cardinal. Il y a B_{n-k} telles partitions.

Par suite,

$$|\mathcal{P}_{n+1,k}| = \binom{n}{k} B_{n-k}$$

et finalement

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_{n-k}$$

Série génératrice exponentielle Pour résoudre cette relation de récurrence, on va s'aider des séries entières. On se doute que le rayon de convergence de la série de terme général B_n est probablement nul, donc on considère plutôt la série génératrice exponentielle associée. Pour montrer que cette dernière a un rayon de convergence non nul, il suffit de remarquer que

$$B_n \leq n!$$

. En effet, à toute partie A de $\{1, \ldots, n\}$ de cardinal k on associe la permutation de $\{1, \ldots, n\}$ formée par le cycle de support A, énuméré par ordre croissant

$$c_A := (a_1, \ldots, a_k) \quad a_1 < \cdots < a_k \in A$$

.

À une partition de $\{1, \ldots, n\}$ on peut donc associer la permutation produit des cycles (à support disjoints car on a une partition !) associés à chaque sous ensemble de la partition. Par unicité de la décomposition en produit de cycles à support disjoint on en déduit que cette application est injective, et par suite

$$B_n \leq |S_n| = n!$$

.

Par conséquent, $\left(\frac{B_n}{n!}\right)$ est bornée, et donc la série entière de terme général $\left(\frac{B_n}{n!}\right)$ a un rayon de convergence au moins 1.

Pour $t < 1$ on note alors

$$S(t) := \sum_{n=0}^{+\infty} \frac{B_n}{n!}$$

Par dérivation terme à terme de S on a pour tout $t \in]-1, 1[$:

$$\begin{aligned} S'(t) = \sum_{n=0}^{\infty} \frac{(n+1)B_{n+1}}{(n+1)!} t^n &= \sum_{n=0}^{+\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} B_{n-k} t^n \\ &= \sum_{n=0}^{+\infty} \sum_{k=0}^{n} \frac{1}{k!} \frac{B_{n-k}}{(n-k)!} t^n \end{aligned}$$

On reconnaît alors le produit de Cauchy de la série entière définissant S et de la série entière exponentielle. Par suite pour tout $t \in]-1, 1[$,

$$S'(t) = S(t) \exp(t)$$

On résout une EDO Puisque $S(0) = B_0 = 1$, S est solution du problème de Cauchy linéaire

$$\begin{cases} y' &= e^t y \\ y(0) &= 1 \end{cases}$$

D'après le *Théorème de Cauchy Lipschitz Linéaire*, ce problème a une unique solution f définie sur tout $\mathbb{R}$ par

$$f(t) := \frac{1}{e} e^{e^x}$$

et S coïncide avec f sur $]-1, 1[$.

On développe f en série entière

$$\exp(\exp(t)) = \sum_{k=0}^{+\infty} \frac{\exp(kt)}{k!} = \sum_{k=0}^{+\infty} \sum_{n=0}^{+\infty} \frac{k^n t^n}{n!k!}$$

Or,

$$\begin{aligned} \sum_{k=0}^{+\infty} \sum_{n=0}^{+\infty} \left| \frac{k^n t^n}{n!k!} \right| &= \sum_{k=0}^{+\infty} \sum_{n=0}^{+\infty} \frac{k^n |t|^n}{n!k!} \\ &= \sum_{k=0}^{+\infty} \frac{\left(e^{|t|}\right)^k}{k!} \\ &= e^{e^{|t|}} < +\infty \end{aligned}$$

Par le *théorème de Fubini* on a donc :

$$\begin{aligned} f(t) &= \frac{1}{e} \sum_{k=0}^{+\infty} \sum_{n=0}^{+\infty} \frac{k^n t^n}{n!k!} \\ &= \frac{1}{e} \sum_{n=0}^{+\infty} \sum_{k=0}^{+\infty} \frac{k^n t^n}{n!k!} \\ &= \sum_{n=0}^{+\infty} \frac{1}{n!} \left(\frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!} \right) t^n \end{aligned}$$

Conclusion f est donc dérivable en série entière sur $]-1, 1[$, et coïncide avec S. Par unicité du DSE, on en déduit

— D'une part que le rayon de convergence de S est $+\infty$

— D'autre part,

$$B_n = \frac{1}{e} \sum_{k=0}^{+\infty} \frac{k^n}{k!}$$

□

02 Algorithme de Berlekamp [Timé]

02.1 Remarques sur le timing

— Juste la preuve de l'algo c'est peut-être un peu court. Je mets 12-13 min pour la faire proprement, sans rusher.

— Si ça arrive le jour de l'oral, il suffit de parler complexité, ce qui est cool ça donne un peu de recul mais faut maitriser la suite.

— Colonne 1 On présente l'objectif qu'on veut atteindre, on pose Φ_P, on précise la linéarité, on présente l'isomorphisme chinois et $Q^q = Q \mod P \Leftrightarrow Q^q = Q \mod P_i$ pour tout i.

— Colonne 2 : Extension de corps, $Q^q - Q = \prod_{s\in\mathbb{F}_q}(Q-s)$ donc $Q \mod P_i$ est constant à s_i pour tout $i \Rightarrow$ La dimension de l'espace vectoriel des points fixes nous donne le nombre de facteurs irréductibles. On traite le cas $r = 1$.

— Colonne 3 on commence $r > 1$, on introduit $T_\alpha = P \wedge (Q - \alpha)$. On factorise T_α.

— Colonne 4, les I_α partitionnent $\{1, \dots, r\}$ et donc on sait factoriser totalement P.

Timing : 15'32 avec la complexité.

02.2 Recasages :

— 123 - Corps Finis. Applications

— 141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

02.3 Références :

— *Objectif Agreg*, Beck [BMP05]

— *Calcul formel*, Picart, Rannou [SPR02]

— *Cours d'algèbre*, Demazure [Dem97]

02.4 Contexte :

Contexte de Berlekamp :

— Polynôme sans facteur carré

— Remontée d'une factorisation dans $Z[X]$, voir [SPR02]

02.5 Développement

Soit p un nombre premier, q une puissance de p et $k := \mathbb{F}_q$ le corps fini à q éléments. On considère un polynôme $P \in \mathbb{F}_q[X]$ sans facteurs carrés qu'on écrit

$$P = \prod_{i=1}^{r} P_i.$$

où les P_i sont irréductibles et premiers entre eux deux à deux. L'algorithme de Berlekamp calcule le nombre r de facteurs irréductibles de P et donne les P_i.

Posons $d := \deg P$

Le lemme Chinois fournit un isomorphisme de $\mathbb{F}_q$ algèbres :

$$\begin{cases} \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P_1) \times \cdots \times \mathbb{F}_q[X]/(P_r) \\ (Q \mod P) & \mapsto & (Q \mod P_1, \ldots, Q \mod P_r) \end{cases}$$

et puisque les P_i sont irréductibles, les quotients $K_i := \mathbb{F}_q[X]/(P_i)$ sont des corps. C'est là qu'on utilise l'hypothèse que P est sans facteurs carrés : La décomposition due au théorème Chinois se fait en r facteurs distincts.

L'idée est de chercher l'ensemble $\mathcal{E}_P$ des polynômes de degré au plus n et invariants par l'élévation à la puissance q.

Considérons l'application $\mathbb{F}_q$ linéaire suivante

$$\Phi_P : \begin{cases} \mathbb{F}_q[X]/(P) & \to & \mathbb{F}_q[X]/(P) \\ Q & \mapsto & Q^q \end{cases}$$

Alors l'ensemble $\mathcal{E}_P = \operatorname{Fix} \Phi_P = \operatorname{Ker}(\Phi_P - Id)$ est un $\mathbb{F}_q$ espace vectoriel de dimension finie.

Par l'isomorphisme chinois,

$$Q \in \mathcal{E}_P \Leftrightarrow Q^q \equiv Q \mod P \Leftrightarrow Q^q \equiv Q \mod P_i \qquad \text{pour tout } i.$$

Or, les K_i sont des extensions de $\mathbb{F}_q$ donc

$$X^q - X = \prod_{\alpha \in \mathbb{F}_q} (X - \alpha)$$

et par suite

$$\begin{aligned} (Q^q \equiv Q \mod P_i) &\Leftrightarrow \prod_{\alpha \in \mathbb{F}_q} (Q - \alpha) \equiv 0 \mod P_i \\ &\Leftrightarrow Q - s_i \equiv 0 \mod P_i \text{ Pour un certain } s_i \in \mathbb{F}_q \text{ (Intégrité)} \end{aligned} \tag{4.1}$$

On en déduit que le théorème chinois fournit un isomorphisme entre $\mathbb{F}_q^r$ et $\mathcal{E}_P$ qui est donc de dimension r.

Si r = 1 Alors P est irréductible et la factorisation est terminée.

Si r ≥ 2 Par (4.1), $Q \in \mathcal{E}_P$ si et seulement s'il existe $(s_1, \ldots, s_r) \in \mathbb{F}_q^r$ tel que $Q \equiv s_i \mod P_i$ pour tout i. Puisque l'ensemble des polynômes de $\mathbb{F}_q[X]$ constants modulo P est une droite vectorielle, et que la dimension de $\mathcal{E}_P$ est strictement supérieure à 1, on peut trouver Q non constant dans $\mathcal{E}_P$.

Fixons $\alpha \in \mathbb{F}_q$. Calculons $P \wedge (Q - \alpha)$.

— Comme $P \wedge (Q - \alpha)$ est un diviseur de P, il existe $I_\alpha \subset \{1, \ldots, r\}$ tel que

$$P \wedge (Q - \alpha) = \prod_{i \in I_\alpha} P_i.$$

Soit $i \in I_\alpha$. Alors $Q \equiv \alpha \mod P_i$ d'une part, et $Q \equiv s_i \mod P_i$ d'autre part. Donc

$$\alpha \equiv s_i \mod P_i$$

Or, α et $s_i \in \mathbb{F}_q$ et par conséquent

$$\alpha = s_i$$

et

$$I_\alpha \subset \{i \mid s_i = \alpha\}.$$

— Réciproquement, si $\alpha = s_i$ alors $P_i \mid Q - \alpha$ et puisque les P_i sont premiers entre eux, le lemme de Gauss assure que

$$\prod_{\{i|s_i=\alpha\}} P_i \mid Q - \alpha.$$

Comme ce produit divise aussi P, on en déduit qu'il divise leur pgcd et par conséquent

$$\{i \mid s_i = \alpha\} \subset I_\alpha.$$

En remarquant que les I_α partitionnent $\{1, \dots, r\}$ lorsque α parcourt $\mathbb{F}_q$ on en déduit finalement que

$$P = \prod_{i=1}^{r} P_i = \prod_{\alpha \in \mathbb{F}_q} \left(\prod_{i \in I_\alpha} P_i \right) = \prod_{\alpha \in \mathbb{F}_q} (P \wedge (Q - \alpha))$$

Ces facteurs $P \wedge (Q - \alpha)$ ne peuvent pas être tous constants car leur produit est de degré $d \geq 1$ et aucun ne peut être associé à P car sinon P diviserait un $Q - \alpha$ qui serait donc nul dans ${}^{\mathbb{F}_q[X]}\!/_{(P)}$, contredisant l'hypothèse faite sur Q. Ainsi, au moins deux d'entre eux sont des facteurs non triviaux de P, et on peut continuer par récurrence.

02.6 L'algorithme

Formater Joliment l'algorithme ?

L'algorithme s'écrit donc de la façon suivante :
On choisit $\mathcal{B} := (1, X, \dots, X^{d-1})$ une base de ${}^{\mathbb{F}_q[X]}\!/_{(P)}$.

1. Calcul de $X^{kq} \mod P$ pour $k = 0, 1, \dots, d-1$ –> d fois le temps d'une division Euclidienne dans $\mathbb{F}_q$ donc $O(d^2)$ opérations.
2. En déduire la matrice de $\Phi_P - Id$ dans la base $\mathcal{B}$.
3. Calculer la dimension de $\mathcal{E}_P := \mathrm{Ker}(\Phi_P - Id)$. –> Il suffit d'échelonner la matrice (via la méthode de Gauss) et de compter le nombre de lignes nulles. Cette étape se fait en $O(d^3)$ opérations.
4. Si la dimension de $\mathcal{E}_P$ est 1 alors renvoyer P, sinon choisir Q non constant dans $\mathcal{E}_P$ et calculer les pgcd $P \wedge (Q - \alpha)$ pour $\alpha \in \mathbb{F}_q$ –> Le calcul d'un pgcd de deux polynômes de degré majoré par d demande $\sim d$ divisions euclidiennes, donc un coût $O(d^2)$ par pgcd. On fait au plus $q - 1$ calculs de pgcd (on s'arrête dès qu'on a un facteur non trivial) donc cette étape se fait en $O(qd^2)$.

Remarque : Pour trouver une base de $\operatorname{Ker} M$ on résout le système linéaire $MX = 0$.

Complexité : Puisqu'il y a au plus d facteurs irréductibles, on peut majorer grossièrement le coût de l'algorithme de Berlekamp à $O(qd^3)$ opérations. Dans le cas où $q = p^n$ est très grand, cet algorithme devient très coûteux. On se limite donc souvent à des petits corps finis ($\mathbb{Z}/p\mathbb{Z}$ pour p premier petit par exemple).

03 Une caractérisation de la fonction Γ

03.1 Recasages :

— 229 - Fonctions monotones. Fonctions convexes. Exemples et applications.
— 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

03.2 Références :

— *Analyse 2*, Chambert-Loir [CLF95]

03.3 Prérequis :

03.4 Développement :

Theorem 03.1. Soit

$$\Gamma : \left\{ \begin{array}{ccc} \mathbb{R}_+^* & \to & \mathbb{R}_+^* \\ s & \mapsto & \int_0^{+\infty} x^{s-1}e^{-x}dx \end{array} \right.$$

Alors Γ est l'unique fonction $f : \mathbb{R}_+^* \to \mathbb{R}_+^*$ telle que :
— $f(x+1) = xf(x)$
— $f(1) = 1$
— $\log f$ est convexe

Démonstration.

1ère étape : Γ est bien définie et vérifie les propriétés

— Soit $s > 0$. Alors $x^{s-1}e^{-x} = o(\frac{1}{x^2})$ donc $\Gamma(s)$ est bien définie et par intégration par partie :

$$\Gamma(s+1) = \int_0^{+\infty} x^s e^{-x}dx = [-x^s e^{-x}]_0^{+\infty} + s\int_0^{+\infty} x^{s-1}e^{-x}dx = s\int_0^{+\infty} x^{s-1}e^{-x}dx = s\Gamma(s)$$

— $\Gamma(1) = \int_0^{+\infty} e^{-x}dx = 1$
— $\Gamma(s) > 0$ pour $s > 0$.
  — Pour $s > 0$, $x \mapsto x^{s-1}e^{-x}$ est mesurable.
  — Pour $x > 0$, $s \mapsto x^{s-1}e^{-x}$ est de classe $\mathcal{C}^2$.
  — Posons $\gamma(x,s) := x^{s-1}e^{-x} = e^{(s-1)\ln(x)-x}$ Alors :

$$\frac{\partial \gamma}{\partial s} = (\ln(x))x^{s-1}e^{-x}$$
$$\frac{\partial^2 \gamma}{\partial s^2} = (\ln(x))^2 x^{s-1}e^{-x}$$

Donc pour $s \in]\varepsilon, M[$,

$$\left|\frac{\partial^j \gamma}{\partial s^j}\right| \leq |(\ln(x))|^j x^{\varepsilon-1} \qquad \text{Si } 0 < x \leq 1$$
$$\left|\frac{\partial^j \gamma}{\partial s^j}\right| \leq |(\ln(x))|^j x^{M-1} e^{-x} \qquad \text{Si } x \geq 1$$

Alors,

$$g(x) := \begin{cases} \dfrac{|\ln(x)|^j}{x^{1-\varepsilon}} & \text{si } 0 < x \leq 1 \\ |\ln(x)|^j x^{M-1} e^{-x} & \text{si } x \geq 1 \end{cases}$$

est intégrable et domine les dérivées de γ.

Donc Γ est $\mathcal{C}^2$. Par composition, $\log \Gamma$ est $\mathcal{C}^2$ et

$$(\log \Gamma)' = \frac{\Gamma'}{\Gamma}$$

puis

$$(\log \Gamma)'' = \frac{\Gamma''\Gamma - \Gamma'^2}{\Gamma^2}$$

On étudie le signe de $\Gamma''\Gamma - \Gamma'^2$:

$$\begin{aligned} \Gamma'(s)^2 &= \left(\int_0^{+\infty} (\ln x) e^{-x} x^{s-1} dx\right)^2 \\ &= \left(\int_0^{+\infty} \left(e^{-x/2} x^{(s-1)/2}\right) \left((\ln x) e^{-x/2} x^{(s-1)/2}\right) dx\right)^2 \\ &\leq \int_0^{+\infty} \left(e^{-x/2} x^{(s-1)/2}\right)^2 dx \int_0^{+\infty} \left((\ln x) e^{-x/2} x^{(s-1)/2}\right)^2 dx \\ &= \int_0^{+\infty} e^{-x} x^{(s-1)} dx \int_0^{+\infty} (\ln x)^2 e^{-x} x^{(s-1)} dx \\ &= \Gamma(s)\Gamma''(s) \end{aligned}$$

D'où $\Gamma(s)\Gamma''(s) - \Gamma'(s) \geq 0$ et par suite $(\log \Gamma)'' \geq 0$ donc $\log \Gamma$ est bien convexe.

2eme étape Unicité :

Soit f vérifiant l'équation fonctionnelle. Alors par récurrence, on prouve que $f(n+1) = n! = \Gamma(n+1)$ pour tout entier n.

$\log f$ est convexe, donc pour tous $x, y > 0$ et tout $t \in [0, 1]$,

$$\begin{aligned} \log f(tx + (1-t)y) &\leq t \log f(x) + (1-t) \log f(y) \\ &= \log\left(f(x)^t f(y)^{1-t}\right) \end{aligned}$$

Par croissance de $u \mapsto \exp(u)$ on a finalement

$$f(tx + (1-t)y) \leq f(x)^t f(y)^{1-t}$$

Soit $x \in]0, 1]$. Alors :

—

$$\begin{aligned} f(x+n) &= f(x(n+1)+(1-x)n) \\ &\leq f(n+1)^x f(n)^{1-x} \\ &= (n!)^x((n-1)!)^{1-x} \\ &= n^x(n-1)! \end{aligned}$$

Or,

$$f(x+n) = (x+n)f(x+n-1) = (x+n)(x+n-1)f(x+n-2) = f(x)\prod_{k=0}^{n-1}(x+k)$$

d'où

$$f(x) \leq \frac{n^x(n-1)!}{\prod_{k=0}^{n-1}(x+k)}$$

— D'autre part,

$$\begin{aligned} n! = f(n+1) &= f(x(n+x)+(1-x)(n+1+x)) \\ &\leq f(n+x)^x f(n+x+1)^{1-x} \\ &= f(n+x)^x f(n+x)^{1-x} \times (n+x)^{1-x} \\ &= (n+x)^{1-x} f(n+x) \\ &= (n+x)^{1-x} f(x)\prod_{k=0}^{n-1}(x+k) \end{aligned}$$

d'où

$$f(x) \geq \frac{n!(n+x)^{x-1}}{\prod_{k=0}^{n-1}(x+k)}$$

Par suite on a l'encadrement suivant :

$$\frac{n!(n+x)^{x-1}}{\prod_{k=0}^{n-1}(x+k)} \leq f(x) \leq \frac{n^x(n-1)!}{\prod_{k=0}^{n-1}(x+k)}$$

Or,

$$\frac{n^x(n-1)!}{\prod(x+k)} \times \frac{\prod(x+k)}{n!(n+x)^{x-1}} = \frac{n^x}{n(n+x)^{x-1}} = \left(\frac{n}{n+x}\right)^{x-1} \to_{n\to\infty} 1$$

Donc

$$\frac{n^x(n-1)!}{\prod(x+k)} \sim_{n\to\infty} f(x)$$

Par le même raisonnement,

$$\frac{n^x(n-1)!}{\prod(x+k)} \sim_{n\to\infty} \Gamma(x)$$

Donc par unicité de la limite,

$$f(x) = \Gamma(x)$$

(pour $x \in]0,1]$).

On étend l'égalité sur $]0, \infty[$ en utilisant l'égalité

$$f(x+1) = xf(x) = x\Gamma(x) = \Gamma(x+1)$$

Finalement,

$$f = \Gamma$$

□

04 Théorème de Cartan Von Neumann

04.1 Remarques sur le timing

— Ne pas faire Lie-Trotter et l'espace vectoriel, mais sinon ça a l'air de rentrer dans le temps imparti.

Timing :

04.2 Recasages :

— 106 - Groupe linéaire d'un espace vctoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

— 156 - Exponentielle de matrices. Applications.

— 214 - Théorème d'inversion locale, théorème des foctions implicites. Exemples et applications en analyse et en géométrie.

04.3 Références :

— Pour une introduction aux sous-variétés

  — *Calcul Différentiel*, Avez [Ave97]

  — *Introduction aux variétés différentielles*, Lafontaine [Laf97]

  — Rouvière [Rou03]

— Pour le développement :

  — *40 développements d'Analyse*, J et L Bernis [Ber18]

  — *Groupes de Lie*, Mneimné - Testard [Mne86]

04.4 Développement

On munit l'espace vectoriel $\mathcal{M}_n(\mathbb{R})$.

Theorem 04.1. Soit $n \in \mathbb{N}^*$ et G un sous-groupe de $GL_n(\mathbb{R})$. Si G est fermé dans $GL_n(\mathbb{R})$, alors G est une sous-variété de $\mathcal{M}_n(\mathbb{R})$.

Remarque : Il faut comprendre sous-variété de $\mathcal{M}_n(\mathbb{R})$ comme sous-variété de $\mathbb{R}^{n^2}$

04.5 Preuve

On va utiliser la définition classique de sous-variété et chercher pour tout $A \in G$ un sous-espace vectoriel E de $\mathcal{M}_n(\mathbb{R})$, un voisinage ouvert U de 0 dans $\mathcal{M}_n(\mathbb{R})$, un voisinage V_A de A dans $\mathcal{M}_n(\mathbb{R})$, et un $\mathcal{C}^1-$difféomorphisme $\varphi_A : U \to V_A$ qui vérifie $\varphi_A(0) = A$ et

$$\varphi_A(U \cap E) = G \cap V_A$$

Réduction du problème

On va montrer qu'on peut se ramener à $A = I_n$. En effet, supposons que le résultat soit vrai pour l'identité, et soit $U, V_{I_n} et \varphi_{I_n}$ comme précédemment. Fixons $A \in G$ et considérons l'opérateur de translation à gauche par A : $t_A(H) := AH$. C'est un isomorphisme, donc en particulier un $\mathcal{C}^1-$difféomorphisme et par suite $V_A := AV_{I_n}$ est un voisinage ouvert de A dans $\mathcal{M}_n(\mathbb{R})$.

Alors l'application $\varphi_A := t_A \circ \varphi_{I_n} : U \to V_A$ est un $\mathcal{C}^1-$difféomorphisme d'un voisinage de 0 sur un voisinage de A tel que $\varphi_A(0) = A$ et

$$\varphi_A(U \cap E) = t_A(G \cap V_{I_n}) = t_A(G) \cap V_A$$

Or, G est laissé stable par t_A puisque c'est un groupe et $A \in G$. Par suite

$$\varphi_A(U \cap E) = G \cap V_A$$

Cas de l'identité

On va utiliser fortement l'exponentielle de matrice et son inverse le logarithme matriciel.

Posons

$$E := \{M \in \mathcal{M}_n(\mathbb{R}) \mid \forall t \in \mathbb{R}, \exp(tM) \in G\}$$

et prouvons que c'est un sev de $\mathcal{M}_n(\mathbb{R})$.

$0 \in E$ et il est stable par homothétie. Toute la difficulté est donc de montrer que E est stable par somme.

Soit $A, B \in E$. Si elles commutaient, on aurait directement pour tout t, $\exp(t(A + B)) = \exp(tA)\exp(tB) \in G$ puisque c'est un groupe.

Dans le cas général, on va exploiter la fermeture de G et trouver une suite de points de G qui converge vers $\exp(t(A + B))$ via la formidable formule de Lie-Trotter-Kato [1] :

$$e^{A+B} = \lim_{k\to\infty} \left[e^{A/k} e^{B/k}\right]^k \tag{4.2}$$

Puisque G est un groupe, pour tout $t \in \mathbb{R}$ et $k \in \mathbb{N}$, $\left[\exp(\frac{tA}{k})\exp(\frac{tB}{k})\right]^k \in G$ et par passage à la limite on en déduit que $e^{t(A+B)} \in G$.

Lie-Trotter-Kato

À partir de là, il y a plusieurs façons de procéder, selon les leçons. Si on a déjà introduit le logarithme matriciel et son développement, on peut tout de suite passer à 4.3 mais dans la leçon sur l'inversion locale autant déterminer un DL

L'exponentielle matricielle est de classe $\mathcal{C}^1$ et sa différentielle en 0 est l'identité qui est bien inversible. En vertu du *Théorème d'inversion locale*, l'application exponentielle définit un $\mathcal{C}^1-$difféomorphisme d'un voisinage U de 0 sur un voisinage ouvert V de l'identité. Notons L son inverse local.

Par différenciation d'une fonction composée, pour tout H tel que $I_n + H \in V$ on en déduit le développement suivant :

1. Voir le sujet d'Analyse de 2017 pour des généralités sur cette formule, mais attention c'est calculatoire

$$\begin{aligned} L(I_n + H) &= L(I_n) + dL(I_n) \cdot H + o(\|H\|) \\ &= (d(exp)(0))^{-1} \cdot H + o(\|H\|) \\ &= H + o(\|H\|) \end{aligned}$$

Soit à présent $t \in \mathbb{R}$. Pour k suffisamment grand

$$\exp(\frac{tA}{k}) \exp(\frac{tB}{k}) = I_n + t\frac{A+B}{k} + o\left(\frac{1}{k}\right) \in V$$

donc en utilisant les propriétés de l'exponentielle de matrice on a

$$\begin{aligned} \left[\exp(\frac{tA}{k}) \exp(\frac{tB}{k})\right]^k &= \left[e^{L\left(\exp(\frac{tA}{k}) \exp(\frac{tB}{k})\right)}\right]^k \\ &= e^{kL\left(I_n + t\frac{A+B}{k} + o\left(\frac{1}{k}\right)\right)} \\ &= e^{t(A+B)+o(1)} \\ &\to e^{t(A+B)} \end{aligned} \tag{4.3}$$

Donc $A + B \in E$ et E est bien un espace vectoriel.

Construction du difféomorphisme

Soit F un supplémentaire de E dans $\mathcal{M}_n(\mathbb{R})$ et définissons l'application

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{M}_n(\mathbb{R}) = E \oplus F & \to & GL_n(\mathbb{R}) \\ X_E + X_F & \mapsto & \exp(X_E) \exp(X_F) \end{array} \right.$$

Alors φ est de classe $\mathcal{C}^1$ comme produit et composée de fonctions $\mathcal{C}^1$ et $\varphi(0) = I_n$.
Par ailleurs pour tout $H \in \mathcal{M}_n(\mathbb{R})$:

$$\begin{aligned} \varphi(0 + H) &= (I_n + H_E + o(\|H_E\|)) (I_n + H_F + o(\|H_F\|)) \\ &= I_n + (H_E + H_F) + o(\|H\|) \\ &= \varphi(0) + H + o(\|H\|) \end{aligned}$$

Donc $d\varphi(0) = I_n$ est inversible, et en réutilisant de nouveau le *Théorème d'inversion locale* on en déduit que φ induit un $\mathcal{C}^1-$difféomorphisme d'un voisinage ouvert U de 0 dans $\mathcal{M}_n(\mathbb{R})$ sur un voisinage ouvert V de I_n.

(U, φ) est bien une carte locale

Par construction, $\varphi(E) \subset G$ et donc

$$\varphi(E \cap U) \subset G \cap V.$$

En fait, on n'a pas forcément l'inclusion réciproque, mais on va voir qu'on peut réduire U pour l'avoir.

En effet, supposons par l'absurde que pour tout voisinage W de 0 inclus dans U il existe $g \in G \cap \varphi(W)$ tel que

$$X := \varphi^{-1}(g) \notin E \cap W \tag{4.4}$$

Soit $r > 0$ tel que $B(0,r) \subset U$. Posons alors pour tout k, $W_k := B(0, \frac{r}{2^k})$. C'est une suite strictement décroissante de voisinages de 0 inclus dans U et

$$\bigcap_{k=0}^{\infty} W_k = \{0\}$$

.

Pour tout k choisissons $g_k \in G \cap \varphi(W_k)$ tels que $X^{(k)} := \varphi^{-1}(g_k)$ vérifient 4.4.

Décomposons $X^{(k)} = X_E^{(k)} + X_F^{(k)}$, avec $X_F^{(k)} \neq 0$ par hypothèse. Puisque $X^{(k)} \in W_k, \quad X_k \to 0$ et par suite $X_F^{(k)} \to 0$.

Posons $Y_k := \dfrac{X_F^{(k)}}{\|X_F^{(k)}\|}$ le normalisé de $X_F^{(k)}$.

Quitte à extraire, on peut supposer que que $Y_k \to Y \in F$ de norme 1.

On va montrer qu'en fait $Y \in E$ et donc par somme directe $Y = 0$ ce qui est absurde.

Fixons $t \in \mathbb{R}$ et posons pour tout k, $\quad e_k := \left\lfloor \dfrac{t}{\|X_F^{(k)}\|} \right\rfloor$ et $f_k \in [0,1[$ la partie fractionnaire. Alors :

$$\begin{aligned} \exp(tY_k) &= \exp((e_k + f_k)X_F^{(k)}) \\ &= \exp(e_k X_F^{(k)}) \exp(f_k X_F^{(k)}) \end{aligned} \tag{4.5}$$

(f_k) étant bornée, $f_k X_F^{(k)} \to 0$ et en passant à la limite dans 4.5 on a

$$\left(\exp(X_F^{(k)})\right)^{e_k} \to \exp(tY)$$

Or,

$$\exp(X_F^{(k)}) = \exp(-X_E^{(k)}) g_k \in G$$

Donc pour tout k

$$\left(\exp(X_F^{(k)})\right)^{e_k} \in G$$

et par fermeture

$$\exp(tY) \in G.$$

et par suite

$$Y \in E.$$

04.6 Conclusion

Donc $Y = 0$ et $\|Y\| = 1$. Absurde.

Par conséquent il existe un voisinage W de 0 tel que :

$$\varphi(E \cap W) = G \cap \varphi(W)$$

Et G est bien une sous variété.

05 Suites à convergence lente [Timé]

05.1 Remarques sur le timing

— Ce dev n'est pas long, et est bas niveau donc le jury peut voir directement les erreurs.

— Attention à bien laisser 5/6 minutes juste pour l'application.

— Colonne 1 on écrit le théorème, on présente la convergence vers 0 de la suite (u_n).

— Colonne 2 on parle de la dérivée discrète, et pourquoi on introduit cette puissance.

— Colonne 3 on obtient l'équivalent, puis on commence l'application. Il faut bien préciser quel est l'exposant qu'on prend.

— Colonne 4 on termine le DL_2. Attention aux erreurs de calcul, ça fait tâche à l'agreg.

Timing : 15'35 (mais j'ai buggué sur le DL à la fin ...)

05.2 Recasages :

— 223 - Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

— 224 - Exemples de développements asymptotiques de suites et de fonctions.

— 226 - Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchée d'équations.

05.3 Références :

— Référence : FGN *Analyse 1* [FN07b]

05.4 Développement

Theorem 05.1. Soit $c > 0$. On note $I := [0, c]$ et on considère $f : I \to I$ une fonction continue. On suppose de plus qu'au voisinage de zéro il existe $r > 1$ et $\lambda > 0$ tels que

$$f(x) = x - \lambda x^r + o(x^r)$$

On pose $u_0 \in I$ et $u_{n+1} = f(u_n)$. Alors, si u_0 est assez petit, la suite (u_n) converge vers zéro et de plus on a l'équivalent suivant :

$$u_n \sim (n\lambda(r-1))^{\frac{1}{1-r}}$$

Et on propose une application :
Etude de la suite définie par récurrence suivante :

$$\begin{cases} u_0 & \in \mathbb{R}^+ \\ u_{n+1} & = \ln(1+u_n) \end{cases}$$

05.5 Preuve

Démonstration. f est continue sur I et par passage à la limite dans le développement limité, $f(x)\underset{x\to 0}{\to}0$ donc $f(0)=0$. De plus, $f(x)-x=-\lambda x^r<0$ donc il existe $\eta>0$ tel que $f(x)<x$ pour $x\in]0,\eta[$.

Si $u_0\in]0,\eta[$ alors (u_n) est décroissante, et positive, donc (u_n) converge, vers un point fixe de f. Donc $u_n\to 0$.

Déterminons un équivalent de u_n

Remarquons que $u_{n+1}=f(u_n)=u_n-\lambda u_n^r+o(u_n^r)$. Donc

$$(u_{n+1}-u_n)u_n^{-r}\sim -\lambda.$$

Posons $g(x):=x^{1-r}$. Alors $g'(x)=(1-r)x^{-r}$ et par suite

$$(u_{n+1}-u_n)g'(u_n)\sim -(1-r)\lambda.$$

Ceci s'apparente à la "dérivée discrète" de $g(u_n)$.

Etudions alors $g(u_{n+1})-g(u_n)$ ie $u_{n+1}^{1-r}-u_n^{1-r}$.

$$\begin{aligned}u_{n+1}^{1-r}&=(u_n-\lambda u_n^r+o(u_n^r))^{1-r}\\&=u_n^{1-r}(1-\lambda u_n^{r-1}+o(u_n^{r-1})^{1-r}\\&=u_n^{1-r}(1-\lambda(1-r)u_n^{r-1}+o(u_n^{r-1}))\end{aligned}$$

Car $u_n\to 0$.

D'où

$$u_{u+1}^{1-r}-u_n^{1-r}=-\lambda(1-r)+o(1)$$

et donc

$$u_{n+1}^{1-r}-u_n^{1-r}=\lambda(r-1)+o(1)$$

On utilise alors le théorème de sommation des relations de comparaisons (positives) pour faire un analogue discret de l'intégration :

$$\begin{aligned}\sum_{k=0}^{n-1}(u_{k+1}^{1-r}-u_k^{1-r})&=u_n^{1-r}-u_0^{1-r}\\&=n\lambda(r-1)+o(n)\end{aligned}$$

D'où

$$u_n\sim(n\lambda(r-1))^{\frac{1}{1-r}}$$

□

Application :

$$\begin{cases} u_0 & \in \mathbb{R}^+ \\ u_{n+1} & = \ln(1+u_n) \end{cases}$$

$f(x) := \ln(1+x) = x - \dfrac{x^2}{2} + o(x^2)$

On est dans le cadre de ce résultat avec $\lambda = \dfrac{1}{2}$ et $r = 2/$

Par ailleurs, pour tout $x \in \mathbb{R}_+^*$; $\ln(1+x) < x$. Pour tout $u_0 \in \mathbb{R}_+^*$, $u_n \to 0$. Par suite :

$$u_n \sim \frac{2}{n}$$

Adaptons la méthode pour chercher un terme de plus :

$$f(x) = x - \frac{x^2}{2} + \frac{x^3}{3} + o(x^3)$$

d'où

$$u_{n+1} = u_n - \frac{u_n^2}{2} + \frac{u_n^3}{3} + o(u_n^3)$$

$$\begin{aligned} u_{n+1}^{-1} &= (u_n - \frac{u_n^2}{2} + \frac{u_n^3}{3} + o(u_n^3))^{-1} \\ &= u_n^{-1}(1 - \frac{u_n}{2} + \frac{u_n^2}{3} + o(u_n^2))^{-1} \\ &= u_n^{-1} + \frac{1}{2} - \frac{u_n}{12} + o(u_n) \end{aligned}$$

D'où

$$u_{n+1}^{-1} - u_n^{-1} - \frac{1}{2} \sim \frac{-u_n}{12} \sim \frac{-1}{6n} \tag{4.6}$$

On rappelle le développement de la somme partielle de la série harmonique :

$$H_n = \ln n + \gamma + o(1)$$

Alors, en sommant dans 4.6 il vient :

$$\begin{aligned} u_n &= (\frac{n}{2} - \frac{1}{6}\ln n + o(\ln n))^{-1} \\ &= \frac{2}{n}(1 - \frac{1}{6}\frac{\ln n}{n} + o(\frac{\ln n}{n}))^{-1} \\ &= \frac{2}{n}(1 + \frac{1}{6}\frac{\ln n}{n} + o(\frac{\ln n}{n})) \end{aligned}$$

Conclusion :

$$u_n = \frac{2}{n} + \frac{2}{3}\frac{\ln n}{n^2} + o(\frac{\ln n}{n^2})$$

06 Formes quadratiques et décomposition polaire [Timé]

06.1 Remarques sur le timing

— Dev un peu long si on n'y fait pas attention.

— Colonne 1 on fait la décomposition polaire et on montre que $M^T \in O(p,q)$.

— Colonne 2 on fait la stabilité par racine carrée, faut essayer d'aller vite là dessus sous peine de ne pas terminer la fin avec les calculs par blocs. Ici on doit être là à 7'.

— Colonne 3 on fait un bilan de la situation. On rappelle que la décomposition polaire est un homéo sur son image, et qu'elle interne à $O(p,q)$. On en déduit que son image est bien dans $(O(n) \cap O(p,q)) \times (S_n^{++} \cap O(p,q))$. La réciproque étant claire, on a un homéo. Mine de rien, cette partie peut faire perdre du temps si on s'étend trop. Pas plus de $2-3$ minutes ici.

— Normalement il reste 5 minutes pour les calculs par blocs, ils vont occuper les colonnes 3 et 4 (une colonne par facteur).

Timing : 17' mais j'ai perdu du temps stupidement sur le bilan provisoire ....

06.2 Recasages :

— 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupe de $GL(E)$. Applications.

— 156 - Exponentielle de matrices. Applications.

— 170 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

06.3 Références :

— *NH2G2-1*, Caldero-Germoni [CG17a]

06.4 Prérequis

Definition 06.1. Soit $p,q \in \mathbb{N}^*$. On note $O(p,q)$ le sous groupe de $GL_{p+q}(\mathbb{R})$ formé des isométries de la forme quadratique de signature (p,q) :

$$q(x) := x_1^2 + \cdots + x_p^2 - x_{p+1}^2 - \cdots - x_{p+q}^2$$

dont la matrice dans la base canonique est

$$I_{p,q} := \begin{pmatrix} I_p & \\ & -I_q \end{pmatrix}$$

.

Notation : Le groupe $O_p(\mathbb{R})$ sera noté $O(p)$.

Theorem 06.2 (Décomposition Polaire)**.** Soit $M \in GL_n(\mathbb{R})$. Alors il existe $O \in O(n), S \in \mathcal{S}_n^{++}(\mathbb{R})$ telles que $M = OS$. De plus, $S = \sqrt{{}^tMM}$ et l'application

$$\begin{array}{ccc} O(n) \times \mathcal{S}_n^{++} & \to & GL_n(\mathbb{R}) \\ (O, S) & \mapsto & OS \end{array}$$

est un homéomorphisme.

Theorem 06.3. L'application $\exp : \mathcal{S}_n(\mathbb{R}) \to \mathcal{S}_n^{++}$ est un homéomorphisme.

Remarque En dimension 2, en identifiant $GL_2(\mathbb{R}) \simeq \mathbb{C}^*$ il s'agit simplement de voir que tout complexe z non nul s'écrit de façon unique comme

$$z = \rho e^{i\theta} \simeq \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} \rho & 0 \\ 0 & \rho \end{pmatrix}.$$

06.5 Développement

Theorem 06.4. Soit $p, q \neq 0$. Il existe un homéomorphisme

$$O(p, q) \simeq O(p) \times O(q) \times \mathbb{R}^{pq}$$

Démonstration. Posons $n = p + q$

1ère étape : Décomposition polaire

$O(p, q) \subset GL_n(\mathbb{R})$, donc admet une décomposition polaire : Pour tout $M \in O(p, q)$, il existe un unique $(O, S) \in O_n(\mathbb{R}) \times S_n^{++}(\mathbb{R})$ tel que $M = OS$ et on a $S^2 = M^TM =: T$. Montrons qu'elle est en réalité interne ie $O, S \in O(p, q)$. Puisque c'est un groupe, il suffit de prouver que $S \in O(p, q)$.

2eme étape : $O(p, q)$ est stable par transposée

$M \in O(p, q)$ ie $MI_{p,q}M^T = I_{p,q}$. On en déduit par passage à l'inverse que $(M^T)^{-1}I_{p,q}M^{-1} = I_{p,q}$ ie $(M^T)^{-1} \in O(p, q)$. Puisque $O(p, q)$ est un groupe on a donc $M^T \in O(p, q)$. Par suite, $T \in O(p, q)$.

3ème étape : $\mathcal{S}_n^{++} \cap O(p, q)$ est stable par racine carrée

Pour montrer la stabilité par racine carrée, on va utiliser l'exponentielle de matrice. Par (06.3), il existe $U \in \mathcal{S}_n(\mathbb{R})$ telle que $T = \exp(U)$, de sorte que $S = \exp\left(\frac{U}{2}\right)$. Alors :

$$\begin{aligned} T \in O(p,q) &\Leftrightarrow T I_{p,q} T^T = I_{p,q} \\ &\Leftrightarrow T^T = I_{p,q}^{-1} T^{-1} I_{p,q} \\ &\Leftrightarrow (\exp U)^T = I_{p,q}^{-1} (\exp U)^{-1} I_{p,q} \\ &\Leftrightarrow \exp(U^T) = I_{p,q}^{-1} \exp(-U) I_{p,q} \\ &\Leftrightarrow \exp(U^T) = \exp(-I_{p,q}^{-1} U I_{p,q}) \end{aligned}$$

Par injectivité de exp et symétrie de U on en déduit

$$T := \exp(U) \in O(p,q) \Leftrightarrow U I_{p,q} + I_{p,q} U = 0$$

Cette condition est linéaire, ce qui va nous permettre de remonter à $S = \exp\left(\frac{U}{2}\right)$:

$$\begin{aligned} T \in O(p,q) &\Leftrightarrow \frac{U}{2} I_{p,q} + I_{p,q} \frac{U}{2} = 0 \\ &\Leftrightarrow \frac{U^T}{2} = -I_{p,q}^{-1} \frac{U}{2} I_{p,q} \\ &\Leftrightarrow \exp\left(\frac{U^T}{2}\right) = \exp\left(-I_{p,q}^{-1} \frac{U}{2} I_{p,q}\right) \\ &\Leftrightarrow \left(\exp\left(\frac{U}{2}\right)\right)^T = I_{p,q}^{-1} \left(\exp\left(\frac{U}{2}\right)\right)^{-1} I_{p,q} \\ T = S^2 \in O(p,q) &\Leftrightarrow S = \exp\left(\frac{U}{2}\right) \in O(p,q) \end{aligned}$$

La dernière ligne étant vraie par unicité de la racine carrée.

4ème étape : On factorise $O(p,q)$ par décomposition polaire

La décomposition polaire induit donc un homéomorphisme

$$O(p,q) \simeq (O(p,q) \cap O(n)) \times \left(O(p,q) \cap \mathcal{S}_n^{++}\right)$$

5ème étape : On étudie les deux facteurs

— Soit $O \in O(p,q) \cap O(n)$. Alors d'une part, $O^T I_{p,q} O = I_{p,q}$ et $O^T O = I_n$ donnent $I_{p,q} O = O I_{p,q}$ ie O commute avec $I_{p,q}$ En écrivant $O := \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ par blocs, on en déduit que $B = C = 0$.
D'autre part,

$$\begin{pmatrix} A & \\ & D \end{pmatrix} \in O(p,q) \Leftrightarrow \left\{ \begin{array}{ll} A^T A & = I_p \\ D^T D & = I_q \end{array} \right.$$

On en déduit que

$$O(p,q) \cap O(n) = \left\{ \begin{pmatrix} A & 0 \\ 0 & D \end{pmatrix}, A \in O(p), D \in O(q) \right\} \simeq O(p) \times O(q)$$

— Pour le second facteur on réutilise l'exponentielle. Posons

$$L := \{U \in \mathcal{M}_n(\mathbb{R})\,,\, UI_{p,q} + I_{p,q}U^T = 0\}$$

On a vu plus haut que l'exponentielle réalise un homéomorphisme

$$\mathcal{S}_n(\mathbb{R}) \cap L \simeq O(p,q) \cap \mathcal{S}_n^{++}$$

Or,

$$U = \begin{pmatrix} A & B \\ B^T & D \end{pmatrix} \in S_n(\mathbb{R}) \cap L \Leftrightarrow 2\begin{pmatrix} A & 0 \\ 0 & -D \end{pmatrix} = 0 \tag{4.7}$$

$$\Leftrightarrow A = D = 0 \tag{4.8}$$

D'où $\dim(\mathcal{S}_n^{++} \cap L) = pq$ et $\mathcal{S}_n^{++} \cap L \simeq \mathbb{R}^{pq}$.

Conclusion :

$$O(p,q) \simeq O(p) \times O(q) \times \mathbb{R}^{pq}$$

□

06.6 Postrequis

Postrequis de la décomposition polaire de $O(p,q)$.

Theorem 06.5. Soit $p, q \in \mathbb{N}$. Alors le groupe $O(p,q)$ est compact ssi $p = 0$ ou $q = 0$.

Theorem 06.6. Le groupe topologique $O(p,q)$ admet quatre composantes connexes.

07 Algorithme pour la décomposition de Dunford

07.1 Recasages :

— 153 - Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie.

— 157 - Endomorphismes trigonalisables. Endomorphismes nilpotents.

07.2 Références :

— *Rombaldi Algèbre*, [Rom17]

07.3 Prérequis

Lemma 07.1. Soient a, b deux endomorphismes qui commutent et tels que a est inversible, et b nilpotent. Alors $a-b$ est inversible. De plus, si a et b sont des polynômes en un endomorphisme u, alors $(a-b)^{-1}$ est un polynôme en u.

Démonstration. $a - b = a(Id - a^{-1}b)$ Or, b est nilpotent et commute avec a. Donc $a^{-1}b$ est nilpotent. On note r son indice de nilpotence. Alors

$$(Id - a^{-1}b)\sum_{k=0}^{r-1}(a^{-1}b)^k = Id - (a^{-1}b)^r)Id$$

Donc $Id - a^{-1}b$ est inversible, et par suite $a - b$ est inversible, d'inverse

$$a\sum_{k=1}^{r-1}(a^{-1}b)^k$$

Si $a, b \in K[u]$ on a bien $(a-b)^{-1} \in K[u]$. □

07.4 Développement

Soit E un $K-$espace vectoriel de dimension finie, et soit $u \in \mathcal{L}$. On suppose que K est algébriquement clos ce qui assure que son polynôme caractéristique χ_u est scindé et s'écrit

$$\chi_u = \prod_{k=1}^{p}(X - \lambda_k)^{\alpha_k}$$

On note $u = d+n$ la décomposition de Dunford de u, avec d diagonalisable, n nilpotente et $dn = nd$ et on pose $P := \prod_{k=1}^{p}(X - \lambda_k)$ le polynôme minimal de d (C'est bien son polynôme minimal car il est scindé à racines simples, unitaire, et a les mêmes racines que $\chi_u = \chi_d$). On sait que $d \in K[u]$. L'idée est de chercher d comme solution de

$$\begin{cases} P(w) = 0 \\ w \in K[u] \end{cases}$$

Pour cela on va utiliser la méthode de Newton en définissant la suite (w_k) de polynômes en u :

$$\begin{cases} w_0 = u \\ w_{k+1} = w_k - P(w_k)\,(P'(w_k))^{-1} \end{cases}$$

On va alors prouver que la suite est bien définie et qu'elle converge vers d.
On prouve par récurrence les points suivants :

(i) w_k est un polynôme en u

(ii) $P'(w_k)$ est inversible et son inverse est un polynôme en u.

(iii) $P(w_k)$ est nilpotent.

Initialisation

(i) $u \in K[u]$

(ii) P est scidé à racines simples, donc P et P' n'ont aucune racine en commun. Par suite, χ_u et P' n'ont donc aucune racine en commun et ils sont donc premiers entre eux. Par le théorème de Bézout il existe U, V tels que

$$U\chi_u + VP' = 1$$

En évaluant cette relation en u et en utilisant le théorème de Cayley-Hamilton, on en déduit que $V(u)P'(u) = Id$ et donc $P'(u)$ est inversible, d'inverse $V(u) \in K[u]$.

(iii) $P(u)^m = P^m(u)$, or

$$P^m = \prod_{k=1}^{p} (X - \lambda_k)^m$$

donc pour $m \geq \max_{1\leq i\leq p} \chi_u \mid P^m$. En particulier $P^m(u) = 0$ et donc $P(u)$ est nilpotent.

Hérédité Supposons le résultat vrai pour $0 \leq j \leq k$.

(i) $w_{k+1} = w_k - P(w_k)(P(w_k))^{-1}$ est alors bien défini et est un polynôme en $w_k \in K[u]$. C'est donc bien un polynôme en u.

(ii) On considère la formule de Taylor (Formelle) : Il existe $Q \in K[X, Y]$ tel que

$$P'(Y) - P'(X) = (X - Y)Q(X, Y)$$

Alors,

$$P'(w_{k+1}) - P'(w_k) = (w_{k+1} - w_k)Q(w_{k+1}, w_k)$$

Or, $w_{k+1} = W_{k+1}(u)$ et $w_k = W_k(u)$ sont tous les deux des polynômes en u. Par suite, $Q(w_{k+1}, w_k) = Q(W_{k+1}(u), W_k(u)) =: R_k(u)$ est un polynôme en u. On en déduit

$$P'(w_{k+1}) - P'(w_k) = -P(w_k)(P'(w_k))^{-1}R_k(u) \in -P(w_k)S_k(u)$$

avec $S_k(u) = (P'(w_k))^{-1}R_k(u)$ est un polynôme en u. Or, par l'hypothèse de récurrence, $P(w_k)$ est un polynôme en u donc commute avec $S_k(u)$. De plus il est nilpotent, donc $-P(w_k)S_k(u)$ est nilpotent.
Par suite, $P'(w_{k+1}) = P'(w_k) - P(w_k)S_k(u)$ est la différence d'un inversible (hypothèse de récurrence) et d'un nilpotent, il est donc inversible et son inverse est un polynôme en u (Lemme 07.1).

(iii) On réutilise la formule de Taylor : Il existe un polynôme $Q \in K[X,Y]$ tel que

$$P(Y) = P(X) + (Y-X)P'(X) + (Y-X)^2 Q(X,Y)$$

En évaluant en (w_k, w_{k+1}) et en utilisant que ce sont deux polynômes en u on obtient l'existence d'un polynôme R_k tel que

$$P(w_{k+1}) = P(w_k) - P'(w_k)(w_{k+1} - w_k) + (w_{k+1} - w_k)^2 R_k(u)$$

. Or,

$$w_{k+1} - w_k = -P(w_k)(P'(w_k))^{-1} = -(P'(w_k))^{-1}(P(w_k)$$

et par suite

$$P(w_{k+1}) = P(w_k) - P(w_k) + (-P(w_k)(P'(w_k))^{-1})^2 R_k(u) \in P(w_k)^2 K[u] \tag{4.9}$$

Puisque $P(w_k)$ est un polynôme en u nilpotent, en on déduit que $P(w_{k+1})$ est bien nilpotent, ce qui conclut la récurrence.

Convergence

La suite est stationnaire D'après (4.9) $P(w_{k+1}) \in P(w_k)^2 K[u]$ et donc par récurrence $P(w_k) \in P(u)^{2^k} K[u]$. Or, $P(u)$ est nilpotent. Donc en un nombre d'étape *logarithmique*, $P(w_k) = 0$ et donc $w_{k+1} = w_k$.

La suite converge vers d On note k_0 l'indice à partir duquel la suite stationne. Alors $P(w_{k_0}) = 0$ et P est scindé à racines simples. Donc w_{k_0} est diagonalisable. Par ailleurs,

$$u - w_{k_0} = w_0 - w_{k_0} = \sum_{j=0}^{k_0-1} w_j - w_{j+1}$$

. Comme chacune des différences est un polynôme en u qui est nilpotent, on en déduit que $u - w_{k_0}$ est nilpotent. Comme w_{k_0} est un polynôme en u on en déduit que u et $u - w_{k_0}$ commutent. On a donc la décomposition

$$u = w_{k_0} + (u - w_{k_0})$$

. Par unicité de la décomposition de Dunford, on en déduit $w_{k_0} = d$ et $u - w_{k_0} = n$.

07.5 Postrequis

Soit n l'indice de nilpotence de $P(u)$. Alors, l'algorithme fait un $O(\log n)$ étapes. A chaque étape on doit calculer $P(w_k)(P'(w_k))^{-1}$.

Donner la complexité avec le calcul de l'inverse via Bezout

08 Alternative de Fredholm [Timé]

08.1 Remarques sur le timing

— Colonne 1 : Dimension finie du noyau.

— Colonne 2 : Fermeture de l'image, peut-être expliciter l'histoire de la distance qui vaut 1 (une ligne de plus pour sortir $\|u_n - v_n\|$).

— Colonne 3 : On présente la suite strictement décroissante de fermés $F_n = (I-T)^n(E)$.

— Colonne 4 : Lemme de Riesz et on conclut.

Timing : 15'49, un peu de temps perdu colonne 3, on peut aller plus vite sur $F_2 \neq F_1$.

08.2 Recasages :

— 203 - Utilisation de la notion de compacité.

— 208 - Espaces vectoriels normés, applications linéaires continues. Exemples.

08.3 Références

— Brézis, p 92-94 [Bré87]

08.4 Contexte

Ce théorème concerne la résolution de l'équation

$$u - Tu = f \tag{4.10}$$

et l'équation homogène associée

$$u - Tu = f \tag{4.11}$$

On a l'alternative suivante :

— Ou bien pour tout f, 4.10 admet une unique solution

— Ou bien 4.11 admet n solutions linéairement indépendantes, et l'équation non homogène est résoluble ssi f vérifie n conditions d'orthogonalité (ie $f \in Ker(I-T^*)^\perp$)

Remark 08.1. La propriété 3 généralise le cas de la dimension finie aux opérateurs $I - T$ où T est compact : Il est injectif ssi il est surjectif.

Lemma 08.2 (de Riesz)**.** Soit E un e.v.n et soit $M \subset E$ un sev fermé tel que $M \neq E$. Alors :

$$\forall \varepsilon > 0 \; \exists u \in E, \; ||u|| = 1, \; dist(u, M) \geq 1 - \varepsilon$$

Proof of. lemma 08.2
Soit $v \in E$, avec $v \notin M$. Comme M est fermé, alors $d = dist(v, M) > 0$. On choisit $m_0 \in M$ tel que

$$d \leq ||v - m_0|| \leq \frac{d}{1-\varepsilon}$$

Alors,

$$u = \frac{v - m_0}{||v - m_0||}$$

convient. En effet, si $m \in M$ on a :

$$\begin{aligned} ||u - m|| &= ||\frac{v - m_0}{||v - m_0||}|| \\ &= \frac{1}{||v - m_0||}||v - (m_0 + ||v - m_0||m)|| \\ &\geq 1 - \varepsilon \end{aligned}$$

puisque $m_0 + ||v - m_0||m \in M$.

08.5 Développement

Soit E un espace de Hilbert. On note $\mathcal{K}(E)$ l'ensemble des opérateurs compacts de E dans lui-même.

Theorem 08.3. Soit $T \in \mathcal{K}(E)$. Alors :

1. $Ker(I - T)$ est de dimension finie
2. $Im(I - T)$ est fermé et plus précisément $Im(I - T) = Ker(I - t^*)^\perp$.
3. $Ker(I - T) = \{0\} \Leftrightarrow Im(I - T) = E$

Démonstration.

1. (1) Soit $E_1 := Ker(I - T)$. Alors $B_{E_1} \subset T(B_E)$. Or, T est un opérateur compact, donc $T(B_E)$ est relativement compact. Par suite B_{E_1} est compacte, et par le théorème de Riesz E_1 est de dimension finie.
2. (2) Soit $f_n := u_n - Tu_n \to f$. On va montrer que $f \in Im(I - T)$. Posons $d_n := dist(u_n, E_1)$. Comme E_1 est de dimension finie, il existe $v_n \in \mathbb{E}_1$ tel que $d_n := ||u_n - v_n||$.
   Comme $v_n \in E_1$; $v_n - Tv_n = 0$ d'où $f_n = (u_n - v_n) - T(u_n - v_n)$.
   Montrons que d_n reste borné. Par l'absurde, s'il existe une sous suite telle que $||u_{n_k} - v_{n_k}|| \to \infty$, posons $w_n := \frac{u_n - v_n}{||u_n - v_n||}$. Alors comme (f_{n_k}) est bornée :

$$w_{n_k} - Tw_{n_k} = \frac{f_{n_k}}{||u_{n_k} - v_{n_k}||} \to 0 \tag{4.12}$$

   Or, $w_n \in B_E$ et T est compact, donc $T(B_E)$ est relativement compact. Quitte à extraire, on peut supposer qu'il existe z, $Tw_{n_k} \to z$ et par 4.12, $w_{n_k} \to z$ aussi. Donc :

$$z \in Ker(I-T) = E_1$$

Or puisque $v_n \in E_1$,

$$dist(w_n, E_1) = \frac{dist(u_n, E_1)}{||u_n - v_n||} = 1$$

En passant à la limite, on a donc $dist(z, E_1) = 1$. Absurde.
Donc, $||u_n - v_n||$ reste borné et comme T est compact, on peut, quitte à extraire, supposer que $T(u_n - v_n) \to \ell$.
Alors,

$$u_n - v_n = f_n + T(u_n - v_n) \to f + \ell$$

On en déduit que par continuité

$$T(u_n - v_n) \to T(f + \ell)$$

et donc par unicité de la limite,

$$\ell = T(f + \ell)$$

.
En posant $g = f + l$ on a alors $g - Tg = f$, ie

$$f \in Im(I-T)$$

qui est donc bien fermé.
Le résultat sur l'orthogonalité est alors vrai.

3. (3)
   - On prouve d'abord l'implication $\Rightarrow$:
     Par l'absurde, supposons que $F_1 := Im(I-T) \neq E_1$. F_1 est un fermé dans un Hilbert, c'est donc un Hilbert, et $T(F_1) \subset F_1$. Donc $T_{|F_1} \in \mathcal{K}(F_1)$, et $F_2 := (I-T)(F_1)$ est alors fermé dans F_1 d'après 2. De plus, $F_2 \neq F_1$ sinon, en prenant $x \in E_1 \backslash F_1$ (qui est non vide par hypothèse), on aurait

     $$(I-T)(x) \in F_2$$

     donc il existerait $u \in F_1$ tel que

     $$(I-T)(u) = (I-T)(x)$$

     et par injectivité de $I-T$ (c'est l'hypothèse), $x = u$. En particulier, x serait à la fois dans F_1 et hors de F_1.
     En posant $F_n := (I-T)^n(E)$ on obtient alors une suite strictement décroissante de fermés. Par le lemme de Riesz (08.2) il existe (u_n) telle que

     $$u_n \in F_n,\ ||u_n|| = 1,\ dist(u_n, F_{n+1}) \geq \frac{1}{2}.$$

     Donc, si $n > m$, $\quad F_{n+1} \subset F_n \subset F_m$ et par conséquent :

     $$w_{m+1} := -(u_n - Tu_n) + (u_m - Tu_m) + (u_n - u_m) \in F_{m+1}$$

Donc

$$\begin{aligned} ||Tu_n - Tu_m|| &= ||-(u_n - Tu_n) + (u_m - Tu_m) + (u_n - u_m)|| \\ &= ||w_{m+1} - u_m|| \\ &\geq d(u_m, F_{m+1}) \\ &\geq \frac{1}{2} \end{aligned}$$

Par suite, (Tu_n) n'admet aucune sous suite convergente donc $T(B_E)$ ne peut pas être relativement compact. C'est absurde car T est un opérateur compact. Donc, $Im(I-T) = E$, ie $I - T$ est surjective.

— Réciproquement, supposons que $Im(I-T) = E$. Alors

$$Ker(I - T^*) = Im(I-T)^\perp = \{0\}.$$

Puisque T^* est compact, on applique le raisonnement précédent à icelui pour avoir $Im(I - T^*) = E'$. Donc

$$Ker(I-T) = Im(I-T^*)^\perp = E'^\perp = \{0\}$$

et $I - T$ est bien injective.

□

09 Théorème de Frobenius-Zolotarev

09.1 Recasages :

— 105 - Groupes des permutations d'un ensemble fini. Applications.

— 108 - Exemples de parties génératrices d'un groupe. Applications.

— 152 - Déterminant. Exemples et applications.

— 162 - Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

09.2 Références :

— *Objectif Agreg*, Beck [BMP05]

— *Rombaldi Algèbre*, Rombaldi [Rom17]

09.3 Comment recaser ce développement

Ce théorème n'a pas beaucoup d'intérêt en soi. En revanche, sa preuve utilise énormément d'éléments du programme d'algèbre, et le jury n'a pas l'air de s'en lasser. Alors mangez-en.

— Dans la leçon 152 on le recase dans une partie sur les propriétés algébriques du déterminant. C'est très intéressant de ne pas oublier ce caractère qui peut être utile, le déterminant n'est pas là que pour calculer des polynômes caractéristiques, pour tester l'inversibilité ou pour faire de l'analyse !

— Dans la leçon 105 ce théorème donne un calcul non trivial de signature. On va vite sur les propriétés du déterminant, on admet le calcul du groupe dérivé, et on fait l'application à la réciprocité quadratique.

— Dans les leçons 108 et 162, il faut s'attarder sur le calcul du groupe dérivé. On prouve de façon nette et propre que GL_n et SL_n sont engendrées par les matrices élémentaires. On dessine le diagramme, on prouve le lemme de factorisation, on admet la partie permutations et on fait l'application à la réciprocité quadratique.

09.4 Développement

Definition 09.1. Soit $n \geq 2$ et K un corps. On appelle matrice de transvection toute matrice de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ où $i \neq j$ et $\lambda \in K$ et $D_i(\alpha) = I_n + (\alpha - 1)E_{i,i}$ avec $\alpha \in K^*$.

Theorem 09.2. Les matrices de transvection engendrent $SL_n(K)$

Démonstration.

Les transvections engendrent un sous-groupe de SL_n En effet, elles sont toutes de déterminant 1.

Action sur les lignes et les colonnes La multiplication à gauche (resp. à droite) par une matrice de transvection $T_{i,j}(\lambda)$ revient à effectuer sur les lignes (resp. les colonnes) l'opération élémentaire $L_i \leftarrow L_i + \lambda L_j$ (resp. $C_j \leftarrow C_i + \lambda C_j$).

Permutation de deux lignes Pour permuter deux lignes il est nécessaire d'introduire un signe -1 puisqu'une transposition est de signature -1. On remarque que la multiplication à gauche de $T_{i,j}(1)T_{j,i}(-1)T_{i,j}(1)$ a pour effets successifs :

1. $L_i \leftarrow L_i + L_j$
2. $L_j \leftarrow L_j - L_i' = L_j - (L_i + L_j) = -L_i$
3. $L_i' \leftarrow L_i' + L_j' = L_i + L_j - L_i = L_j$

On a donc fait l'opération

$$(L_i, L_j) \leftarrow (L_j, -L_i)$$

Soit $A \in SL_n(K)$. En appliquant l'algorithme du pivot de Gauss nous allons nous ramener à l'identité en n'utilisant que des transvections. Comme A est inversible, sa première colonne n'est pas nulle. Si $a_{i,1} \neq 0$, l'opération $L_1 \leftarrow L_1 - \dfrac{a_{11}-1}{a_{i1}} L_i$ permet de mettre un 1 en position $(1,1)$. Si tous les coefficients a_{i1} pour $i \geq 2$ sont nuls, on effectue l'echange des lignes $(L_1, L_2) \leftarrow (L_2, -L_1)$ pour se ramener au cas précédent.

On utilise $(1,1)$ comme pivot et une succession d'opérations sur les lignes, puis sur les colonnes pour arriver à

$$A \sim \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}$$

Et on recommence l'opération sur A'. Notons qu'on ne touche alors plus à L_1 ou C_1. Par récurrence on obtient une matrice $Diag(1, 1, \dots, 1, \alpha)$ mais puisque nos opérations conservent le déterminant, nécessairement $\alpha = 1$ et on obtient l'identité. On a donc prouvé qu'il existait une suite $M_1, \dots, M_p$ et $N_1, \dots, N_q$ de transvections telles que

$$M_1 \cdots M_p A N_1 \cdots N_q = I_n$$

. Puisque l'inverse d'une transvection est une transvection, on en déduit que A est un produit de transvections. □

Lemma 09.3. Deux matrices de transvections sont conjuguées dans $GL_n(K)$.

Démonstration. Une matrice de transvection est de la forme $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$. Il suffit de prouver que les $E_{i,j}$ sont conjuguées, ie qu'il existe une matrice M telle que pour tout i, j, il existe une base $B_{i,j}$ tel que l'endomorphisme $u_{i,j}$ attaché à $E_{i,j}$ ait M comme matrice.

Soit donc u l'endomorphisme associé à $E_{i,j}$ dans la base canonique. u est de rang 1, et est nilpotent d'indice 2. Soit e_{n-1} une base de l'image. On la complète en une base du

noyau $(e_1, \dots, e_{n-1})$. Soit e_n un antécédent de e_{n-1}. $e_n \notin Ker(u)$ qui est un hyperplan, par suite $(e_1, \dots, e_n)$ est une base de $\mathbb{R}^n$. Dans cette base,

$$mat(u) = \begin{pmatrix} 0 & \dots & 0 & 0 \\ & \ddots & & \vdots \\ & & \ddots & 1 \\ & & & 0 \end{pmatrix}$$

Par suite, dans la base $(e_1, \dots, e_{n-1} = u(e_n), \frac{1}{\lambda}e_n)$, l'endomorphisme attaché à $T_{i,j}(\lambda) = I_n + \lambda E_{i,j}$ a pour matrice

$$\begin{pmatrix} 1 & \dots & 0 & 0 \\ & \ddots & & \vdots \\ & & \ddots & 1 \\ & & & 1 \end{pmatrix}$$

□

Theorem 09.4. $D(GL_n(k)) = SL_n(k)$ sauf si $n = 2$ et $k = \mathbb{F}_2$.

Démonstration. — On élimine le cas trivial $n = 1$. Soit donc $n \geq 2$

— Soit $u, v \in GL_n(K)$. Alors, $\det(uvu^{-1}v^{-1}) = 1$ donc $D(GL_n(K)) \subset SL_n(K)$.

— Supposons $n \geq 3$. Alors $SL_n(K)$ est engendré par les matrices de transvections $T_{i,j}(\lambda)$. Or, elles sont toutes conjuguées à

$$T_n = \begin{pmatrix} I_{n-3} & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} I_{n-3} & 0 \\ 0 & T_3 \end{pmatrix}$$

Il suffit de prouver que T_n est un commutateur. En effet, si $T_n = [A, B]$ alors $T_{i,j}(\lambda) = PT_nP^{-1} = P[A, B]P^{-1} = [PAP^{-1}, PBP^{-1}]$ est alors aussi un commutateur. Par suite, $\langle T_{i,j}(\lambda)\rangle \subset D(GL_n(K))$ ie $SL_n(K) \subset D(GL_n(K))$.
On note

$$A_3 := \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B_3 := \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Alors $A_3, B_3 \in SL_3(\mathbb{K})$ et

$$A_3B_3A_3^{-1}B_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = T_3$$

Par suite, en posant $A_n := \begin{pmatrix} I_{n-3} & 0 \\ 0 & A_3 \end{pmatrix}$ et $B_n = \begin{pmatrix} I_{n-3} & 0 \\ 0 & A_n \end{pmatrix}$ on a bien $T_n = [A_n, B_n]$. D'où le résultat.

— Si maintenant $n = 2$. Les transvections sont conjuguées à $T_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Pour $\lambda, \mu \in K^*$, on a dans $GL_2(K)$:

$$\begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & \mu(\lambda - 1) \\ 0 & 1 \end{pmatrix}$$

Si $K \neq \mathbb{F}_2$ alors on peut choisir $\lambda \in K \backslash \{0, 1\}$ de sorte que λ et $\lambda - 1$ soient inversibles. On pose alors $\mu := (\lambda - 1)^{-1}$, de sorte que T_2 soit bien un commutateur. On conclut comme précédemment que $SL_2(K) \subset D(GL_2(K))$.

□

Theorem 09.5. Soit p un nombre premier impair, et $u \in GL_n(\mathbb{F}_p)$.

$$\varepsilon(u) = \left(\frac{\det u}{p} \right)$$

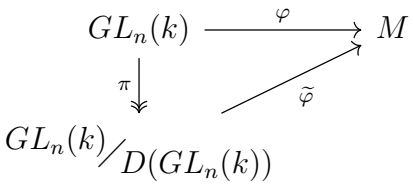
09.5 Preuve

Démonstration.

Propriétés algébriques du déterminant

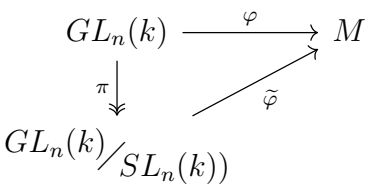
Lemma 09.6. Soit k un corps, M un groupe abélien avec $k \neq \mathbb{F}_2$ ou $n > 2$. Pour tout morphisme de groupes $\varphi : GL_n(k) \to M$ il existe un unique morphisme $\delta : k^\times \to M$ tel que $\varphi = \delta \circ det$.

Démonstration. On utilise la propriété universelle du groupe dérivé : Tout morphisme d'un groupe G dans un groupe abélien se factorise par le groupe dérivé : Il existe un unique morphisme $\widetilde{\varphi}$ tel que $\varphi = \widetilde{\varphi} \circ \pi$ où π est la surjection canonique de sorte à rendre le diagramme suivant commutatif

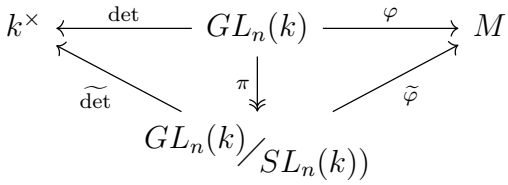


Calcul du groupe dérivé de GL_n On utilise ici le théorème 09.4 **(Qu'on démontre pour les leçons 162 et 108. Il faut absolument y passer du temps.)**

Le diagramme précédent se réécrit donc



Par ailleurs, comme det est un morphisme surjectif de $GL_n(k)$ dans $k^\times$ de noyau $SL_n(k)$, par le théorème d'isomorphisme, il existe un unique isomorphisme $\widetilde{\det}$ tel que $\det = \widetilde{\det} \circ \pi$



Il suffit de remonter les flèches en posant $\delta := \widetilde{\varphi} \circ \widetilde{\det}^{-1}$ pour avoir le résultat. □

Il existe un unique morphisme non trivial

Lemma 09.7. Le symbole de Legendre est l'unique morphisme non trivial de $\mathbb{F}_p^\times$ vers $\{-1, 1\}$.

Démonstration. — Le symbole de Legendre est bien un morphisme de groupe non trivial.

— Réciproquement, soit $\alpha : \mathbb{F}_p^\times \to \{-1, 1\}$ un morphisme non trivial. Comme $\mathbb{F}_p^\times$ est un groupe cyclique, donc engendré par un élément $\omega \in \mathbb{F}_p$ vérifiant $\alpha(\omega) = -1$ car $\alpha \neq 1$. Alors, pour tout carré, $x = y^2 = \omega^{2k}$, $\alpha(x) = \alpha(\omega)^{2k} = 1$. En revanche, si x n'est pas un carré, alors $x = \omega^{2k+1}$, et donc $\alpha(x) = -1$.

□

Calcul de signature

On pose $k = \mathbb{F}_{p^n}$ le corps fini à p^n éléments. La signature est un morphisme de $GL_n(k)$ sur $\{-1, 1\}$ qui est abélien. Donc il se factorise par le déterminant : Il existe un unique morphisme $\delta : k^\times \to \{-1, 1\}$ tel que $\varepsilon = \delta \circ \det$. Il suffit donc de prouver que δ est non trivial. Il suffit de trouver une bijection $\mathbb{F}_p-$ linéaire de k de signature -1. Soit ω un générateur de $k^\times$, et considérons la permutation donnée par $x \mapsto \omega x$. Celle-ci agit alors comme le $p^n - 1$ cycle $(\omega, \omega^2, \ldots, \omega^{p^n-1})$ (qui fixe 0). Or, p^n est impair, donc la signature de ce cycle vaut $(-1)^{p^n-1+1} = -1$. D'où le résultat. □

09.6 Application : Loi de réciprocité quadratique

Réciprocité quadratique dans Frobenius-Zolotarev

Theorem 09.8. Soit p un nombre premier impair.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Démonstration. Soit u l'automorphisme du $\mathbb{F}_p$-espace vectoriel de dimension 1 $\mathbb{F}_p$, défini par $u(x) = 2x$. Alors $det(u) = 2$ et donc par le théorème de Frobenius-Zolotarev,

$$\left(\frac{2}{p}\right) = \varepsilon(u)$$

Il s'agit de calculer la signature de

$$u = \begin{pmatrix} 0 & 1 & \cdots & \frac{p-1}{2} & \frac{p+1}{2} & \frac{p+3}{2} & \cdots & p-2 & p-1 \\ 0 & 2 & \cdots & p-1 & 1 & 3 & \cdots & p-4 & p-2 \end{pmatrix}$$

Soit $N(u)$ le nombre d'inversions de u. Alors $\varepsilon(u) = (-1)^{N(u)}$.

$$N(u) = card \bigsqcup_{i=0}^{\frac{p-1}{2}} \left\{ \left(i, \frac{p+1}{2}\right), \ldots, \left(i, i-1+\frac{p+1}{2}\right) \right\}$$

D'où

$$\begin{aligned} N(u) &= \sum_{i=1}^{\frac{p-1}{2}} i = \frac{1}{2}\left(\frac{p-1}{2}\frac{p+1}{2}\right) \\ &= \frac{p^2-1}{8} \end{aligned}$$

Finalement, on a bien

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

□

10 Invariants de similitude et réduction de Frobenius [Timé]

10.1 Remarques sur le timing

— On vire l'unicité, on ne fait que l'existence. Dans la leçon dualité, on peut peut-être plus s'appesentir sur la dualité.

— Sans l'unicité, ça passe très bien en 15 minutes sans se dépêcher.

— Si jamais il reste trop de temps, bah on regarde l'interpretation matricielle.

Timing : 15' sans l'unicité.

10.2 Recasages :

— 151 - Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.

— 153 - Polynômes d'endomorphismes en dimension finie. Réduction d'un endomorphisme en dimension finie.

— 159 - Formes linéaires et dualité en dimension finie. Exemples et applications.

10.3 Références :

— *Réduction des endomorphismes*, Mneimné-Mansuy [MM12] pour tout le contexte autour

— *Algèbre*, Gourdon [Gou09] pour le développement en utilisant la dualité.

10.4 Contexte

L'objectif est de caractériser l'action par conjugaison du groupe $GL(E)$ sur $\mathcal{L}(E)$. On va en effet attribuer à chaque endomorphisme f une suite de polynômes $P_1, \dots, P_r$ qui ne dépendent que de f et telle que deux endomorphismes sont semblables si et seulement s'ils ont la même suite de polynômes. Cette suite sera alors appelée suite des *Invariants de Similitude* de f.

Les invariants de similitudes fournissent alors un cadre très agréable pour faire de la réduction, et sont en quelque sorte la réduction la plus poussée que l'on peut faire.

Avantages :

— Ne dépend pas du corps

— Pas de détermination de valeurs propres

Algorithme ?

Le lecteur intéressé par une méthode effective pourra lire l'article "Un algorithme pour la décomposition en espaces cycliques" de Bernard Randé dans la RMS 115-4 paru en Mai 2005 [Ran05]

10.5 Prérequis

Soit E un $K-$ev de dimension finie.

Definition 10.1 (Polynôme minimal ponctuel)**.** Pour $x \in E$ et $f \in \mathcal{L}(E)$ il existe un polynôme unitaire $\mu_{f,x}$ de plus bas degré tel que $\mu_{f,x}(f)(x) = 0$.

Definition 10.2 (Sous-espaces cyclique)**.** Pour $x \in E$ et $f \in \mathcal{L}(E)$ on appelle sous-espace cyclique de f engendré par x, et on note $E_{f,x}$ le plus petit sev de E stable par f et contenant x. Cet espace est engendré par la famille $(f^j(x))_{j\in\mathbb{N}}$ et si $p = deg(\mu_{f,x})$ alors $\dim E_{f,x} = p$ et $(x, f(x), \dots, f^{p-1}(x))$ en est une base.

Theorem 10.3. Soit $f \in \mathcal{L}(E)$. Alors il existe $x \in E$ tel que $\mu_{f,x} = \mu_f$.

Démonstration. On décompose le polynôme minimal de f en produit de facteurs irréductibles

$$\mu_f = \prod_{k=1}^{p} P_k^{\alpha_k}.$$

Alors par le lemme des noyaux

$$E = \bigoplus_{k=1}^{p} \ker P_k^{\alpha_k}(f).$$

On vérifie que la suite $(\ker P_k^{\alpha_k}(f))$ est strictement croissante puis stationnaire, et si $x_k \in \ker P_k^{\alpha_k}(f) \setminus \ker P_k^{\alpha_k-1}(f)$ alors $\mu_{f,x_k} = P_k^{\alpha_k}$. Posons $x := x_1 + \dots + x_p$. Alors

$$0 = \mu_{f,x}(f)(x) = \sum_{k=1}^{p} \mu_{f,x}(f)(x_k)$$

Et donc par somme directe, $\mu_{f,x}(f)(x_k) = 0$ pour tout k. Donc $P_k^{\alpha_k}$ divise $\mu_{f,x}$. Puisqu'ils sont premiers entre eux, μ_f divise $\mu_{f,x}$. Or, $deg\mu_f \geq \mu_{f,x}$ et donc $\mu_{f,x} = \mu_f$. □

Definition 10.4. Un endomorphisme f de E est dit cyclique s'il existe x tel que $E = E_{f,x}$.

10.6 Développement

On admet le théorème 10.3.

Theorem 10.5 (Invariants de Similitudes)**.** Soit E un $K-$ espace vectoriel de dimension finie, et $f \in \mathcal{L}(E)$. Il existe une unique suite de polynômes $P_1, \dots, P_r$ et une décomposition

$$E = \bigoplus_{i=1}^{r} F_i$$

telles que

— Pour tout $i \in \{1, \dots, r\}$, $P_{i+1} \mid P_i$

— Pour tout $i \in \{1, \dots, r\}$, la restriction $f_i = f_{|F_i}$ de f à F_i est cyclique de polynôme minimal P_i.

Démonstration.

Existence : On prouve d'abord l'existence, par récurrence sur la dimension n de E. On utilisera un peu de dualité.

— Si $n = 1$ tous les endomorphismes sont cycliques et l'existence est évidente.

— Supposons le résultat vrai pour les endomorphismes d'espaces vectoriels de dimension inférieure ou égale à n. Soit E un $K-$ev de dimension $n+1$ et $f \in \mathcal{L}(E)$. Si f est cyclique, c'est gagné. Sinon on pose $k := deg(\mu_f)$ et soit x tel que $\mu_f = \mu_{f,x}$. Alors $E_{f,x}$ est de dimension $k < n$ et est stable par f.

On cherche un supplémentaire stable On pose

$$e_1 = x, e_2 := f(x), \dots, e_k := f^{k-1}(x)$$

qui forment une base de $F := E_x$, qu'on complète en une base $(e_1, \dots, e_n)$ de E. Soit

$$G := \Gamma^\circ \text{ où } \Gamma := \{e_k^* \circ f^i \mid i \in \mathbb{N}\}.$$

Γ est stable par ${}^t f$ et par dualité G est donc stable par f.

Montrons $F \cap G = \{0\}$ Soit $y \in F \cap G$.
Alors $e_j^*(y) = 0$ si $j > k$ car $y \in F$. De plus, comme $y \in G$, $e_k^*(y) = e_k^*(f^0(y)) = 0$. Par récurrence, en composant par f à la bonne puissance on annule toutes les composantes de y. Donc $y = 0$.

Montrons $\dim F + \dim G = n$ Par dualité, $\dim G = n - \dim Vect\Gamma$. Il suffit de prouver que $\dim Vect\Gamma = k$. Pour cela on considère l'application linéaire

$$\varphi : \left\{ \begin{array}{rcl} K[f] & \to & Vect\Gamma \\ g & \mapsto & e_k^* \circ g \end{array} \right.$$

Par définition de $Vect\Gamma$, φ est surjective. De plus elle est injective : Si $g = \sum_{i=1}^k a_i f^{i-1} \in \ker \varphi$, alors $0 = e_k^*(g)(f(x)) = e_k^*(a_1 e_1 + \dots + a_k e_k) = a_k$. Par récurrence, en composant par f^i on arrive à annuler tous les coefficients et par suite $g = 0$. Donc $\dim Vect\Gamma = k$ et par suite $E = F \oplus G$. Soit $P_1 := \mu_f = \mu_{f_{|F}}$ et $P_2 := \mu_{f_{|G}}$. Comme G est stable par f on en déduit que $P_2 \mid P_1$. On enfin l'hypothèse de récurrence à $f_{|G}$.

Unicité : Supposons qu'il existe deux suites de polynômes distinctes $P_1, \dots, P_r$ et $Q_1, \dots, Q_s$ et considérons les décompositions associées

$$E = \bigoplus_{i=1}^{r} F_i = \bigoplus_{i=1}^{s} G_i.$$

Par construction, $P_1 = Q_1 = \mu_f$ et $\dim F_i = degP_i$, $\dim G_i = degQ_i$.

Alors

$$\sum_{i=1}^{r} \dim F_i = \sum_{i=1}^{s} \dim G_i$$

donc il existe au moins un indice $j \in \{2, \min r, s\}$ tel que $P_j \neq Q_j$. On prend j minimal. Alors :

— Pour $i \leq j-1$, f_{F_i} et f_{G_i} sont cycliques de même polynôme minimal donc sont semblables, et donc $P_j(f_{|F_i})$ et $P_j(f_{|G_i})$ sont semblables. En particulier,

$$\dim P_j(f)(F_i) = \dim P_j(f)(G_i) \tag{4.13}$$

— Puisque F_i est stable par f et $P_i \mid P_j$ pour $i \geq j$, on en déduit que

$$P_j(f)(E) = \bigoplus_{i=1}^{j-1} P_j(f)(F_i) = \bigoplus_{i=1}^{s} P_j(f)(G_i) \tag{4.14}$$

En passant à la dimension dans 4.14 et en utilisant 4.13 on en déduit donc :

$$0 = \sum_{i=j}^{s} \dim P_j(f)(G_i)$$

et par suite $\dim P_j(f)(G_i) = 0$ pour $i \geq j$. En particulier, $P_j(f_{|G_j}) = 0$ ie $Q_j \mid P_j$. Par symétrie, on en déduit que $Q_j = P_j$. Absurde par définition de j. □

10.7 Conclusion

Si $f \in \mathcal{L}(E)$, alors il existe une unique suite finie de polynômes unitaires $P_1, \ldots, P_r$ tels que

— Pour tout i, P_{i+1} divise P_i

— Il existe une base de E dans laquelle la matrice de f est diagonale par blocs et les blocs diagonaux sont les matrices compagnons des polynômes $P_1, \ldots, P_r$

$$\begin{pmatrix} C_{P_1} & & & \\ & C_{P_2} & & \\ & & \ddots & \\ & & & C_{P_r} \end{pmatrix}$$

11 Inversion de Fourier dans $S(\mathbb{R})$

Références : ZQ [ZQ13]

11.1 Prérequis

Definition 11.1. Pour $f \in L^1$, on définit sa transformée de Fourier

$$\hat{f}(t) := \int_{\mathbb{R}} e^{-itx} f(x) dx$$

Theorem 11.2. Si $f \in S(\mathbb{R})$ alors $\hat{f} \in S(\mathbb{R})$

11.2 Développement

On calcule la transformée de Fourier d'une Gaussienne :

Theorem 11.3. Si $f(x) = e^{-x^2}$ alors $\hat{f}(t) = \sqrt{\pi} e^{-t^2/4}$

Puis on en déduit un théorème d'inversion dans la classe de Schwartz :

Theorem 11.4. Si $f \in S(\mathbb{R})$, alors

$$f(x) := \frac{1}{2\pi} \int_{\mathbb{R}} e^{itx} \hat{f}(t) dt$$

11.3 Preuve

Proof of. 11.3 Pour $z \in \mathbb{C}$ on pose

$$F(z) := \int_{\mathbb{R}} e^{zx} e^{-x^2} dx$$

Alors

- Pour tout $x \in \mathbb{R}$, $z \mapsto e^{zx} e^{-x^2}$ est holomorphe sur $\mathbb{C}$.
- Pour tout $z \in \mathbb{C}$, $x \mapsto e^{zx} e^{-x^2}$ est mesurable.
- Si K est un compact de $\mathbb{C}$, soit R tel que $K \subset B(0, R)$.

$$|e^{zx-x^2}| = e^{x\Re(z)-x^2}$$

Donc pour $z \in K$:

- Si $|x| \geq 2R$, $|x\Re(z)| - |x^2| \leq |x|R - |x|^2 \leq -\frac{1}{2}|x|^2$
- Si $|x| \leq 2R$, alors $|x\Re(z)| - |x|^2 \leq 2R^2$

Posons alors

$$g(x) := \begin{cases} e^{-x^2/2} & \text{Si } |x| \geq 2R \\ \\ e^{2R^2} & \text{Si } |x| \leq 2R \end{cases}$$

g est intégrable, indépendant de z et pour $z \in K$, $|e^{zx-x^2}| \leq g(x)$

Donc par le théorème d'holomorphie sous l'intégrale, F est holomorphe sur $\mathbb{C}$.
Or, si $z \in \mathbb{R}$, on a par un changement de variable dans l'intégrale

$$F(z) = \int_{\mathbb{R}} e^{-(x-z/2)^2+z^2/4} dx = e^{z^2/4} \int_{\mathbb{R}} e^{-y^2} dy$$

ie

$$F(z) = \sqrt{\pi} e^{z^2/4}, \text{ Pour } z \in \mathbb{R} \tag{4.15}$$

Puisque $z \mapsto \sqrt{\pi} e^{z^2/4}$ est holomorphe sur $\mathbb{C}$ et coïncide avec F holomorphe sur $\mathbb{R}$, alors d'après le théorème du prolongement analytique, l'égalité 4.15 est vraie sur $\mathbb{C}$ tout entier.

En particulier :

$$\hat{f}(t) = F(-it) = \sqrt{\pi} e^{-t^2/4}$$

Proof of. 11.4 Soit $\varepsilon > 0$. L'idée est d'introduire un paramètre dépendant de ε, qui tend vers 1 lorsque $\varepsilon \to 0$ et dont on va saoir calculer la limite de l'intégrale.

Posons

$$I_\varepsilon(x) := \frac{1}{2\pi} \int_{\mathbb{R}} e^{itx} e^{-\varepsilon t^2} \hat{f}(t) dt$$

D'une part

$$|e^{itx} e^{-\varepsilon t^2} \hat{f}(t)| \leq |\hat{f}(t)| \in L^1$$

car $\hat{f} \in S(\mathbb{R})$,

donc par le Théorème de Convergence Dominée,

$$I_\varepsilon(x) \underset{\varepsilon \to 0}{\to} \frac{1}{2\pi} \int_{\mathbb{R}} e^{itx} \hat{f}(t) dt$$

D'autre part,

$$I_\varepsilon(x) = \frac{1}{2\pi} \int_{\mathbb{R}} e^{itx} e^{-\varepsilon t^2} \left(\int_{\mathbb{R}} e^{-ty} f(y) dy \right) dt$$

Or,

$$\int_{\mathbb{R}} \int_{\mathbb{R}} \left| e^{it(x-y)} e^{-\varepsilon t^2} f(y) \right| dy dt = \left(\int_{\mathbb{R}} e^{-\varepsilon t^2} dt \right) \left(\int_{\mathbb{R}} |f(y)| \, dy \right) < \infty$$

Donc pour tout réel x,

$$(t, y) \mapsto e^{itx} e^{-\varepsilon t^2} e^{-ity} f(y) \in L(\mathbb{R} \times \mathbb{R})$$

. On peut donc appliquer le théorème de Fubini-Lebesgue et par suite

$$I_\varepsilon(x) = \frac{1}{2\pi}\int_{\mathbb{R}} f(y)\left(\int_{\mathbb{R}} e^{-it(y-x)}e^{-\varepsilon t^2}dt\right)dy$$

Faisons le changement de variable $u = \sqrt{\varepsilon}t$, $du = \sqrt{\varepsilon}dt$ Alors :

$$\begin{aligned}\int_{\mathbb{R}} e^{-it(y-x)}e^{-\varepsilon t^2}dt &= \frac{1}{\sqrt{\varepsilon}}\int_{\mathbb{R}} e^{-i\frac{u}{\sqrt{\varepsilon}}(y-x)}e^{-u^2}du \\ &= \frac{1}{\sqrt{\varepsilon}}F\left(\frac{-i(y-x)}{\sqrt{\varepsilon}}\right) \\ &= \frac{1}{\sqrt{\varepsilon}}\sqrt{\pi}e^{-\frac{(y-x)^2}{4\varepsilon}}\end{aligned}$$

D'où

$$I_\varepsilon(x) = \frac{1}{2\pi}\sqrt{\frac{\pi}{\varepsilon}}\int_{\mathbb{R}} f(y)e^{-\frac{(y-x)^2}{4\varepsilon}}dy$$

En faisant le changement de variable $u = \dfrac{y-x}{2\sqrt{\varepsilon}}$ on obtient donc :

$$I_\varepsilon(x) = \frac{1}{\sqrt{\pi}}\int_{\mathbb{R}} e^{-u^2}f(x+2\sqrt{\varepsilon}u)du$$

À nouveau par convergence dominée,

$$I_\varepsilon(x) \to \frac{1}{\sqrt{\pi}}\int_{\mathbb{R}} e^{-u^2}f(x)du$$

Et en utilisant la valeur de l'intégrale de Gauss 4.16 :

$$I_\varepsilon(x) \to f(x)$$

Conclusion : Par unicité de la limite on a donc :

$$f(x) = \frac{1}{2\pi}\int_{\mathbb{R}} e^{itx}\hat{f}(t)dt$$

12 Isométries du cube et représentations de $\mathfrak{S}_4$

12.1 Recasages :

— 101 - Groupe opérant sur un ensemble. Exemples et applications.

— 104 - Groupes finis. Exemples et applications.

— 105 - Groupes des permutations d'un ensemble fini. Applications.

— 183 - Utilisation des groupes en géométrie.

12.2 Références :

— *H2G2*, Caldero-Germoni [CG13]

— *Rombaldi Algèbre*, Rombaldi [Rom17]

— *NH2G2-2*, Caldero-Germoni [CG17b]

12.3 Contexte

Le groupe des isométries (affines) d'une partie de $\mathbb{R}^d$ mesure ses symétries en plus d'avoir une structure de groupe. C'est une notion intéressante en soi, mais qui a aussi un intérêt historiques. En effet, les *groupes de transformations* sont les premiers groupes que les mathématiciens ont considéré, et ce bien avant de formaliser la notion même de groupe.

— L'objet symétrique par excellence est la sphère euclidienne. Elle est laissée invariante par toutes les isométries.

— Lorsque la partie est un polytope convexe régulier, enveloppe convexe de ses points extrêmaux appelés les sommets, ce groupe d'isométries s'identifie à un groupe de permutations. En considérant un polytope à n sommets, on obtient ainsi une *représentation* du groupe des permutations $\mathfrak{S}_n$ dans $\mathbb{R}^d$. Et c'est très utilisé en crystallographie (*Groupe d'espace* d'un cristal). On peut ainsi mettre en commun les deux points de vue duaux :

  — D'une part, une étude géométrique permet d'obtenir des informations sur le groupe des permutations d'un ensemble fini.

  — D'autre part, une étude algébrique de ce même groupe de permutations permet d'obtenir des informations sur les configurations possibles.

Chercher références pour ça

12.4 Prérequis

Soit $\mathcal{E}$ un espace affine euclidien. On suppose choisie une base affine de sorte que $\mathcal{E}$ est identifié à l'espace euclidien $\mathbb{R}^d$.

Definition 12.1. Soit $X \subset \mathbb{R}^d$ une partie à au moins 2 éléments. Le groupe $Is(X)$ (resp. $Is^+(X)$, $Is^-(X)$) des isométries (resp. des déplacements, des anti-déplacements) de X est le groupe formé par toutes les isométries (resp. isométries positives, isométries négatives) g de $\mathbb{R}^d$ telles que $g(X) = X$.

Theorem 12.2. Soit φ une similitude (= composée d'une homothétie et d'une translation = application affine qui multiplie les distances par un facteur constant). Alors on a l'isomorphisme

$$\begin{array}{ccc} Is(X) & \to & Is(\varphi(X)) \\ g & \mapsto & \varphi g \varphi^{-1} \end{array}$$

. En particulier, le groupe des similitudes est le normalisateur du groupe des isométries dans le groupe Affine.

Quitte à composer par une similitude, pour étudier les isométries d'un cube quelconque dans $\mathbb{R}^3$, on peut se limiter à étudier les isométries du cube unité de sommets de coordonnées $(\pm 1, \pm 1, \pm 1)$.

Theorem 12.3. Soit X une partie finie de $\mathbb{R}^3$.

(i) Si X possède un centre de symétrie O et $g \in Is(X)$ alors $g(O) = O$. De plus on a un isomorphisme $Is(X) \simeq Is^+(X) \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

(ii) Si X est stable par une réflexion orthogonale, alors $Is(X) \simeq Is^+(X) \rtimes {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$.

Démonstration. (i) Soit O un centre de symétrie de X, et s_O la symétrie de centre O. Alors $s_O \in Is(X)$. En dim 3, s_O est une isométrie indirecte de X. Puisqu'une application affine préserve l'isobarycentre, on en déduit que s_O fixe l'isobarycentre de X. Par unicité du point fixe de s_O, on en déduit que O est l'isobarycentre de X. Par suite, toute isométrie $g \in Is(X)$ fixe O. Puisque la partie linéaire de s_O est $-Id$ qui est centrale, et que s_O a un point fixe en commun avec toutes les isométries de X on en déduit que s_O est centrale dans $Is(X)$. Alors l'application

$$F : \left\{ \begin{array}{ccc} Is(X) & \to & Is^+(X) \times {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \\ g & \mapsto & \left\{ \begin{array}{ll} (g, 1) & \text{si } g \in Is^+(X) \\ (gs_O, s_O) & \text{sinon} \end{array} \right. \end{array} \right.$$

est un isomorphisme de groupes.

(ii) En toute généralité, on a donc la suite exacte

$$1 \to Is^+(X) \to Is(X) \xrightarrow{\det} \{\pm 1\} \to 1.$$

Or, $Is^+(X) \lhd Is(X)$ est d'indice 2, donc ${}^{Is(X)}\!/_{Is^+(X)} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}} \simeq \{\pm 1\}$. Soit s une réflexion (hyperplane) qui préserve X. Alors elle est d'ordre 2 et le groupe $H := \{Id, s\}$ est aussi isomorphe à ${}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$. Par ailleurs, det réalise un isomorphisme entre H et $\{\pm 1\}$. On a donc

$$Is(X) \simeq Is^+(X) \rtimes {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$$

□

Sur les représentations

Je ne fais que des représentations complexes, et la notions de caractères qui va avec. Il faut connaître les théorèmes de base, orthogonalité des caractères, irréductibilité. De même il faut connaître $\mathfrak{S}_4$.

Theorem 12.4. $\mathfrak{S}_4$ possède exactement 5 classes de conjugaisons :

- La classe de l'identité, de cardinal 1.
- La classe des transpositions, de cardinal 6.
- La classe des 3-cycles, de cardinal 8.
- La classe des doubles transposition, de cardinal 3.
- La classe des 4-cycles, de cardinal 6.

Theorem 12.5. Les seules représentations complexes de degré 1 de $\mathfrak{S}_n$ sont la triviale et la signature. Elles sont irréductibles (car de degré 1).

Theorem 12.6. $\mathfrak{S}_n$ possède une représentation irréductible de degré $n-1$, qu'on appelle représentation standard.

Démonstration. — Soit $(e_1, \dots, e_n)$ la base canonique de $\mathbb{R}^n$. L'action de $\mathfrak{S}_n$ sur les indices, induit une représentation de degré n de $\mathfrak{S}_n$ via les matrices de permutation. Notons χ_{Perm} son caractère. Or, la droite $D := \text{Vect}(e_1 + \cdots + e_n)$ est stable, et l'action de $\mathfrak{S}_n$ y est triviale. Soit $H := D^\perp = \{x \in \mathbb{R}^n \mid x_1 + \cdots + x_n = 0\}$ son hyperplan. Il est aussi stable par l'action de $\mathfrak{S}_n$. Ceci définit alors la *représentation standard* de $\mathfrak{S}_n$, de degré $n-1$.

— Soit χ_{Std} son caractère. Alors pour $\sigma \in \mathfrak{S}_n$,

$$\chi_{Std}(\sigma) = \chi_{Perm}(\sigma) - \chi_{Triv}(\sigma) = Tr(P_\sigma) - 1 = |\{i \mid \sigma(i) = i\}| - 1.$$

Pour montrer son irréductibilité, on va calculer sa norme par un argument probabiliste[2] :

$$\|\chi_{Std}\|^2 = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |\operatorname{Fix}(\sigma) - 1|^2$$

On va alors faire intervenir les probabilités : Soit $\sigma \sim \mathcal{U}_{\mathfrak{S}_n}$ et soit $X_i := \mathbb{1}_{\sigma(i)=i}$ la variable de Bernouilli qui vaut 1 si σ fixe i et 0 sinon. Posons enfin

$$X := \sum_{i=1}^{n} X_i = |\operatorname{Fix}(\sigma)|$$

le nombre total de points fixes. Alors par linéarité,

$$\mathbb{E}(X) = \sum_i \mathbb{E}(X_i) = \sum_i \mathbb{P}(X_i = 1)$$

2. [CG17b] utilise un argument de double transitivité

or, une permutation qui fixe i réalise exactement une permutation des $n-1$ éléments restants. En particulier, $|\{\sigma \in \mathfrak{S}_n \mid \sigma(i) = i\}| = (n-1)!$ et par suite, $X_i \sim B(1/n)$. On en déduit que $\mathbb{E}(X) = 1$. Par ailleurs,

$$Var(X) = \mathbb{E}\left((X - \mathbb{E}(X))^2\right) = \mathbb{E}\left((|\operatorname{Fix}(\sigma) - 1)^2\right) = \frac{1}{n!}\sum_{\sigma\in\mathfrak{S}_n}(|\operatorname{Fix}(\sigma)|-1)^2 = \|\chi_{Std}\|^2$$

Il suffit donc de calculer la variance de X. Or,

$$Var(X) = \sum_i Var(X_i) + 2\sum_{i<j} Cov(X_i, X_j)$$

D'une part, $Var(X_i) = \frac{1}{n}\left(1 - \frac{1}{n}\right)$, d'autre part, $\mathbb{E}(X_iX_j) = \mathbb{E}(\mathbb{1}_{\sigma=i,\sigma=j}) = \mathbb{P}(\sigma = i, \sigma = j) = \frac{(n-2)!}{n!} = \frac{1}{n(n-1)}$, donc

$$Cov(X_i, X_j) = \mathbb{E}(X_iX_j) - \mathbb{E}(X_i)\mathbb{E}(X_j) = \frac{1}{n(n-1)} - \frac{1}{n^2} = \frac{1}{n^2(n-1)}$$

Finalement,

$$\|\chi_{Std}\|^2 = Var(X) = n \times \frac{1}{n}\left(1 - \frac{1}{n}\right) + 2\frac{n(n-1)}{2}\frac{1}{n^2(n-1)} = 1$$

Et par conséquent la représentation standard est toujours irréductible.

□

Remarque : La représentation produit $\varepsilon \times$ Standard est encore une représentation irréductible, de degré $n-1$.

12.5 Développement

Soit C_6 le cube unité de $\mathbb{R}^3$.

Theorem 12.7. On a l'isomorphisme $Is^+(C_6) \simeq \mathfrak{S}_4$. C'est une représentation irréductible de degré 3 de $\mathfrak{S}_4$ différente de la standard. On en déduit la table des caractères de $\mathfrak{S}_4$.

Démonstration.

Schéma d'un cube

1ère étape : On se limite aux isométries qui conservent les sommets

En effet, soit S la sphère de centre 0 et de rayon $\sqrt{3}$ et soit V l'ensemble des sommets de C_6. Alors $V = C_6 \cap S$ donc si $\varphi \in Is(C_6)$,

$$\varphi(V) = \varphi(C_6) \cap \varphi(S) = C_6 \cap S = V.$$

Par conséquent, les isométries qui conservent C_6 conservent les sommets. Réciproquement, une isométrie qui conserve V conserve son enveloppe convexe, et par suite conserve C_6. On a donc

$$Is(C_6) = Is(V).$$

On en déduit que les isométries réalisent une permutation des 8 sommets, et donc

$$Is(X) \hookrightarrow \mathfrak{S}_8.$$

2ème étape : $\mathbf{Is^+(C_6)}$ agit sur les grandes diagonales

Une isométrie conserve les distances. Puisque les grandes diagonales du cube (au nombre de 4) représentent les plus grandes distances possibles entre deux sommets du cube, elles sont laissées globalement invariantes par l'action de $Is(C_6)$, donc de $Is^+(C_6)$. Notons $\mathcal{D} := \{D_1, D_2, D_3, D_4\}$ avec $D_i = [A_iB_i]$ les 4 grandes diagonales. Cette action définit alors un morphisme de groupes

$$\varphi : \left\{ \begin{array}{ccc} Is^+(C_6) & \to & \mathfrak{S}_4 \\ g & \mapsto & g_{|\mathcal{D}} \end{array} \right.$$

3ème étape : L'action est fidèle

— S'il existe i tel que g fixe A_i (et donc aussi B_i). Sans perte de généralité on peut supposer que $i = 1$. Alors puisque g conserve les distances, et $A_1A_2 \neq A_1B_2$, nécessairement g fixe A_2, et donc fixe aussi B_2. De même, A_4 est envoyé sur lui-même. Par conséquent, g fixe le repère affine (A_1, A_2, B_2, A_4). On en déduit que $g = Id_{\mathbb{R}^3}$.

— Soit $g \in \ker \varphi$. Puisque g stabilise la diagonale $D_i = [A_iB_i]$ alors soit elle laisse fixe A_i et B_i, soit elle les permute. Supposons qu'il existe i tel que $g \cdot A_i = B_i$. Alors $s_Og \cdot A_i$ où s_O désigne la symétrie centrale du cube. Alors, par le cas précédent $s_0g = Id_{R^3}$, ce qui est impossible puisque $g \in Is^+$.

On en déduit que

$$Is^+(C_6) \hookrightarrow \mathfrak{S}_4.$$

4ème étape : φ est surjectif

Puisqu'elles engendrent $\mathfrak{S}_4$, il suffit de voir que toutes les transpositions sont réalisées. Or, la rotation d'angle π autour de l'axe reliant les milieux de $[A_iA_{i+1}]$ et $[B_iB_{i+1}]$ réalise la transposition des diagonales D_i, D_{i+1} et fixe les deux autres.

Finalement on obtient une représentation de $\mathfrak{S}_4$ de degré 3

$$Is^+(C_6) \simeq \mathfrak{S}_4.$$

Dictionnaire de cet isomorphisme et table des caractères de $\mathfrak{S}_4$

Afin d'obtenir la table des caractères, on peut dresser la correspondance entre les isométries positives du cube et les permutations associées dans $\mathfrak{S}_4$. On rappelle que $\mathfrak{S}_4$ possède 5 classes de conjugaison. Comme ce sont toutes des rotations, les traces (qui correspondent à l'image de la permutation par le caractère associé) sont toutes de la forme

$1 + 2\cos(\theta)$. Pour les doubles transpositions, on remarque qu'elles sont toutes obtenues comme carré d'un 4-cycle.

$\mathfrak{S}_4$	Cardinal de la classe	$Is^+(C_6)$	Trace
Id	1	Id	3
transposition	6	Rotation d'angle π d'axe passant par les milieux de deux arêtes opposées	-1
3-cycle	8	Rotation d'angle $2\pi/3$ d'axe une grande diagonale	0
4-cycle	6	Rotation d'angle $\pi/2$ d'axe passant par le centre de deux faces opposées	1
Double-transposition	3	Carré de la précédente : Rotation d'angle π d'axe passant par le centre de deux faces opposées	-1

Le caractère associé est donc de norme $\frac{1}{4!}(3^2+6\times(-1)^2+8\times 0^2+6\times 1^2+3\times(-1)^2) = 1$ et est donc irréductible. Par ailleurs, en multipliant par la représentation signature, on retrouve une autre représentation irréductible de degré 3 : C'est la représentation standard, ie l'action par permutation sur les sommets du simplexe de dimension 3, ou encore du tétraèdre dans $\mathbb{R}^3$.

Puisque les seules représentations de $\mathfrak{S}_4$ de degré 1 sont la triviale et la signature, toutes les autres sont de degré au moins 2. Or, $1^2 + 1^2 + 3^2 + 3^2 = 20 = 24 - 2^2$ on en déduit qu'il existe une seule autre représentation irréductible, et elle est de degré 2. On la note θ. Pour obtenir sa ligne, on procède par orthogonalité des colonnes.

On peut alors écrire la table des caractères de $\mathfrak{S}_4$.

Type	Id	(12)	(12)(34)	(123)	(1234)
Cardinal de la classe	1	6	3	8	6
χ_{Triv}	1	1	1	1	1
χ_ε	1	-1	1	1	-1
χ_{Cube}	3	-1	-1	0	1
$\chi_\varepsilon\chi_{Cube} = \chi_{Std}$	3	1	-1	0	-1
χ_θ	2	0	2	-1	0

□

12.6 Postrequis

Les tables des caractères de $\mathfrak{S}_3$ et $\mathfrak{S}_4$ peuvent s'obtenir directement à partir des théorèmes (12.5) et (12.6) et par orthogonalité des caractères pour avoir la représentation de degré 2 de $\mathfrak{S}_4$. On donne ici la table de $\mathfrak{S}_3$:

$\mathfrak{S}_3$	Id	(12)	(123)
Cardinal de la classe	1	3	2
χ_{Triv}	1	1	1
χ_ε	1	-1	1
χ_{Std}	2	0	-1

Donner l'interprétation de la représentation de degré 2 via le quotient par Klein.

13 Méthode de Jacobi (Recherche d'éléments propres)

13.1 Références :

— [CL06]

— [Rom99]

— [Ser02]

13.2 Contexte

Le problème de la détermination des valeurs propres et vecteurs propres d'une matrice est en général bien plus difficile que de résoudre un système linéaire. Plusieurs méthodes sont possibles :

— Des méthodes directes, en calculant le polynôme caractéristique (en général très coûteux mais peut être simple dans certains cas particuliers), puis en approchant ses racines

— Des méthodes itératives, qui sont celles utilisées en pratique.

Mais les méthodes itératives peuvent être plus ou moins efficaces selon les situations.

Quelques exemples :

— La méthode de la *puissance itérée* qui permet de calculer la valeur propre de module maximale de matrices réelles sous certaines conditions. En itérant le processus on peut en déduire les autres valeurs propres lorsque leurs modules sont tous distincts. Mais cette méthode est peu performante en général pour calculer l'ensemble des valeurs propres.

— D'autres méthodes reposent sur un principe d'approximation : Etant donnée une matrice A dont on cherche les éléments propres, on construit une suite (A_k) de matrices semblables à A et qui converge vers une matrice très simple :

  — *Jacobi* : Converge vers une matrice diagonale

  — *Givens-Householder* : Converge vers une matrice tridiagonale

  — *Rutishauser* : Converge vers une matrice triangulaire

Plusieurs problèmes se posent alors pour les méthodes itératives :

— Savoir calculer simplement chaque étape de récurrence : $A_k \to A_{k+1}$

— Stabilité numérique : On veut que les valeurs propres soient bien conservées en pratique

Dans ce développement, je propose une étude de la *méthode de Jacobi* pour les matrices symétriques.

13.3 Description de la méthode

Dans toute la suite, on supposera la dimension $n \geq 2$ et la norme considérée sera la norme subordonée à la norme euclidienne sur $\mathbb{R}^n$:

$$\|M\|^2 := \sum_{i,j} |M_{i,j}|^2.$$

Soit A une matrice symétrique. Par le *Théorème Spectral*, il existe O orthogonale telle que $O^T AO$ soit diagonale. Le principe de la méthode va être de construire une suite de matrices de rotations $(R(\theta_k))$ qui va permettre d'approcher ces matrices orthogonales. On définit la suite (A_k) de la façon suivante :

$$\begin{cases} A_0 &= A \\ A_{k+1} &= \Omega_k^T A_k \Omega_k \end{cases}$$

Le principe de chaque itération est d'annuler deux éléments hors diagonaux en position symétrique $a_{pq}^{(k)}$ et $a_{qp}^{(k)}$. Le choix de p, q est décrit plus bas (13.6)

13.4 Une première remarque

Soit

$$\Omega_{p,q}(\theta) := \begin{pmatrix} I_{p-1} & 0 & 0 \\ 0 & \rho_{p,q}(\theta) & 0 \\ 0 & 0 & I_{n-q} \end{pmatrix}$$

Avec

$$\rho_{p,q}(\theta) := \begin{pmatrix} \cos(\theta) & 0 & -\sin(\theta) \\ 0 & I_{q-p+1} & 0 \\ \sin(\theta) & 0 & \cos(\theta) \end{pmatrix}$$

Lemma 13.1.
Si A est symétrique et $B := \Omega_{p,q}(\theta)^T A \Omega_{p,q}(\theta)$ alors B est aussi symétrique et

$$\sum_{i,j} b_{ij}^2 = \sum_{i,j} A_{i,j}^2$$

Preuve : $\Omega_{p,q}(\theta)$ est orthogonale.

13.5 Choix de θ :

Lemma 13.2. 1. Si $a_{p,q} \neq 0$,

$$\exists! \theta \in I :=]-\frac{\pi}{4}, 0[\cup]0, \frac{\pi}{4}[\quad b_{pq} = 0$$

2. Dans ce cas
$$\sum_i b_{ii}^2 = \sum_i a_{ii}^2 + 2a_{pq}^2$$

Preuve : Soit $e := (e_1, \ldots, e_n)$ la base canonique de $\mathbb{R}^n$. $\Omega_{p,q}$ représente une rotation d'angle θ dans le plan (e_p, e_q). Alors

$$\begin{pmatrix} b_{pp} & b_{pq} \\ b_{qp} & b_{qq} \end{pmatrix} = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} a_{pp} & a_{pq} \\ a_{qp} & a_{qq} \end{pmatrix} \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix}$$

et alors
$$b_{pp}^2 + b_{qq}^2 + 2b_{pq}^2 = a_{pp}^2 + a_{qq}^2 + 2a_{pq}^2$$

Et, par symétrie,

$$\begin{aligned} b_{pq} = b_{qp} &= \begin{pmatrix} \cos(\theta)a_{pp} - \sin(\theta)a_{pq} & \cos(\theta)a_{pq} - \sin(\theta)a_{qq} \end{pmatrix} \begin{pmatrix} \sin(\theta) \\ \cos(\theta) \end{pmatrix} \\ &= a_{pq}\cos(2\theta) + \sin(2\theta)\frac{a_{pp} - a_{qq}}{2} \end{aligned}$$

Alors,

$$b_{pq} = 0 \Leftrightarrow \cos(2\theta) = \sin(2\theta)\frac{a_{qq} - a_{pp}}{2a_{pq}}$$

Cette équation admet une unique solution dans I :

$$\theta = \frac{1}{2} cotg^{-1}\left(\frac{a_{qq} - a_{pp}}{2a_{pp}}\right)$$

Alors
$$a_{pp}^2 + a_{qq}^2 + 2a_{pq}^2 = b_{pp}^2 + b_{qq}^2$$

et puisque les autres coefficients ne sont pas changés,

$$\sum_i b_{ii}^2 = \sum_i a_{ii}^2 + 2a_{pq}^2$$

13.6 Choix de p,q

Pour la méthode de Jacobi, on choisit p, q de sorte que

$$|a_{pq}^{(k)}| = \max_{i \neq j} |a_{i,j}^{(k)}|$$

Theorem 13.3. La méthode de Jacobi converge

Démonstration. Posons $A_k := B_k + D_k$ avec $D_k := Diag(a_{ii}^{(k)})$.

1ère étape : $B_k \to 0$: Posons $\varepsilon_k := \|B_k\|^2$.

Alors par ce qui précède,

$$\varepsilon_{k+1} = \sum_{i\neq j} |a_{ij}^{(k+1)}|^2 = \sum_{i\neq j} |a_{ij}^{(k)}|^2 - |a_{pq}^{(k)}|^2 - |a_{qp}^{(k)}|^2 = \varepsilon_k - 2|a_{pq}^{(k)}|^2.$$

Par ailleurs, compte tenu du choix de p, q,

$$|\varepsilon_k| \leq n(n-1)|a_{pq}^{(k)}|^2$$

et donc

$$|a_{pq}^{(k)}|^2 \geq \frac{\varepsilon_k}{n(n-1)}$$

On en déduit que

$$\varepsilon_{k+1} \leq \varepsilon_k \left(1 - \frac{2}{n(n-1)}\right) \to 0$$

2eme étape : (D_k) est de Cauchy : Rappelons qu'à chaque étape on ne modifie que les entrées ayant au moins un indice dans $\{p, q\}$. Autrement dit, si $i \notin \{p, q\}, a_{ii}^{(k+1)} = a_{ii}^{(k+1)}$. De plus, en posant $t = \tan(\theta_k)$ on a

$$\begin{cases} a_{pp}^{(k+1)} &= a_{pp}^{(k)} - t a_{pq}^{(k)} \\ a_{qq}^{(k+1)} &= a_{qq}^{(k)} + t a_{pq}^{(k)} \end{cases}$$

Remarque : Ne pas faire les calculs ci-dessous à l'oral En effet, notons $c = \cos(\theta_k)$, $s = \sin(\theta_k)$ de sorte que $t = cs$. Alors,

$$a_{pp}^{(k+1)} = c^2 a_{pp}^{(k)} + s^2 a_{qq}^{(k)} - 2cs a_{pq}^{(k)}$$

. Posons

$$X = a_{pp}^{(k+1)} - a_{pp}^{(k)}$$

et laissons tomber les exposants. Notons enfin $x := cotan(2\theta) = \frac{a_{qq} - a_{pp}}{2a_{pq}}$ Alors $x = \frac{c^2 - s^2}{2cs} = \frac{1 - t^2}{2t}$ et

$$\begin{aligned} X &= (c^2 - 1)a_{pp} + s^2 a_{qq} - 2cs a_{pq} \\ &= s^2(a_{qq} - a_{pp}) - 2cs a_{pq} \\ &= -2a_{pq}(cs - s^2 x) \\ &= -2a_{pq}(c^2 t - c^2 t^2 x) \\ &= -2a_{pq}c^2(t - t^2 x) \\ &= -2a_{pq}c^2(t - t^2 \frac{1 - t^2}{2t}) \\ &= -a_{pq}c^2 t(2 - 1 + t^2) \\ &= -a_{pq}c^2 t(1 + t^2) \end{aligned}$$

Or, $c^2 = \frac{1}{1 + t^2}$ d'où finalement $X = -t a_{pq}$ L'autre cas se traite de la même façon.

Retour à l'étape 2 Par suite $D_{k+1} - D_k = Diag(0, \dots, -t_k a_{pq}^{(k)}, 0, \dots, 0, t_k a_{pq}^{(k)}, 0, \dots, 0)$ et par suite

$$\|D_{k+1} - D_k\|^2 = 2t_k^2 |a_{pq}^{(k)}|^2$$

Puisque $|\theta_k| \leq \frac{\pi}{4}$ par construction, $|t_k| \leq 1$ et

$$2|a_{pq}^{(k)}|^2 \leq \|B_k\|^2 \leq \rho^{2k} \|B_0\|^2$$

où $\rho = (1 - \frac{2}{n(n-1)}) < 1$.

On en déduit que (D_k) est de Cauchy, donc converge. On note Δ sa limite.

Δ a les mêmes valeurs propres que A Pour tout k, D_k est diagonale donc Δ est aussi diagonale. Par ailleurs, $B_k \to 0$ et donc $A_k \to \Delta$. Par continuité de l'application $M \mapsto \chi_M$ on en déduit que $\chi_{A_k} \to \chi_\Delta$. Or, A_k est semblable à A et par suite, $\chi_{A_{k)}}$ est constant à χ_A. On en déduit

$$\chi_\Delta = \chi_A.$$

Or Δ est diagonale, donc il existe une permutation σ telle que $\Delta = diag(\lambda_{\sigma(i)})$.

Conclusion On a donc trouvé une suite de matrices semblables à A qui converge vers la matrice diagonale Δ. Par suite, Δ est l'ensemble des valeurs propres de A.

□

13.7 Postrequis

On a le théorème suivant :

> **Theorem 13.4.** Si les valeurs propres de A sont toutes distinctes, alors la suite Ω_k construite dans la méthode de Jacobi converge vers une matrice orthogonale O dont les colonnes constituent un ensemble orthonormal de vecteurs propres de la matrice A.

14 Sous-Groupes compacts de $GL_n(R)$ [Timé]

14.1 Remarques sur le timing

— Dev assez long si on fait tout.

— Ne pas trop se concentrer sur le début du lemme (On insiste sur la compacité, et la stricte convexité de la norme euclidienne, et c'est tout). On donne l'unicité du minimum a et on vérifie que $u(a)$ vérifie encore ce minimum unique pour tout u dans H ce qui donne $u(a) = a$ pour tout u par unicité du minimum. On n'écrit pas forcément beaucoup : Une colonne 1/2, maximum 2.

— On passe à l'action de G sur $S(E)$ par congruence. Attention à conserver les notations du plan. On peut poser $V = S(E)$ pour simplifier. On présente les deux points de vue des actions : Morphisme, et opération explicite, et on montre qu'on est à l'aise pour jongler entre ces deux notions.

— On introduit H comme l'image du morphisme définissant l'action. Comme l'action est continue (même affine), H va être un sous groupe (morphisme), compact (continuité) de $GL(V)$. On introduit alors C comme l'orbite de l'identité par G sous cette action. C'est une partie compacte incluse dans $S^{++}(E)$, et la stabilité par H est claire puisque stable par H = stable par l'action de G et C est précisément une orbite ! (on gagne du temps par rapport au Rombaldi en disant ça, en plus on comprend mieux pourquoi ça marche).

— On énonce le problème : La partie n'est pas convexe. Pour pallier à ça, on prend l'enveloppe convexe, et on invoque le théorème de Carathéodory pour prouver la compacité. Ce nouveau compact K est maintenant un convexe, compact, toujours inclus dans $S^{++}(E)$ puisque ce dernier est convexe, et toujours stable par H puisque l'action est affine donc conserve les barycentres.

— Enfin on applique le lemme pour trouver un point fixe. Puisqu'on est dans les endomorphismes DSP, ce point fixe admet une racine carrée. Selon le temps, on peut faire une pause pour laisser au jury le temps de suivre tout ce qu'on a fait. Enfin, on termine tranquillement pour prouver que notre groupe G est conjugué à $O(E)$.

Timing : 15'30

14.2 Recasages :

— 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

— 203 - Utilisation de la notion de compacité.

14.3 Références

— Rombaldi [Rom17]

14.4 Prérequis

Theorem 14.1. Pour E un espace Euclidien de dimension $n \geq 1$, $O(E)$ est un sous-groupe compact de $GL(E)$.

Theorem 14.2 (Caratheodory)**.** Soit E un $\mathbb{R}-$espace vectoriel de dimension finie n, et soit A une partie de E. Alors, si $x \in Conv(A)$, x est combinaison convexe d'**au-plus** $n+1$ points de A.

Preuve de Caratheodory

Corollary 14.3. En dimension finie, l'enveloppe convexe d'un compact est compacte.

Remark 14.4. Cas d'un groupe fini Si G est un sous groupe fini de $GL(E)$, alors en moyennant le produit scalaire de E par G comme dans la preuve du théorème de $Maschke$, on obtient un produit sclaire rendant tous les éléments de G orthogonaux. D'après la classification des formes quadratiques, ce produit scalaire définit une forme quadratique q congruent à la norme euclidienne sur E. Alors $O(q)$ est conjugué à $O(E)$ et par suite G est conjugué à un sous groupe de $O(E)$.

Mais mieux, la matrice de q dans une base base est une matrice symétrique définie positive, laissée fixe par l'action de G par congruence ! C'est cette idée qu'on va exploiter dans le cas général.

14.5 Développement

Lemma 14.5 (Kakutani)**.** Soit $(V, \|.\|)$ un espace vectoriel normé euclidien, H un sous-groupe compact de $GL(V)$ et K un convexe, compact, non vide de V stable par tous les éléments de H. Alors K admet un élément fixé par toutes les applications de H.

Après avoir démontré ce théorème de point fixe, on va prouver le résultat suivant

Theorem 14.6. Soit $(E, ||.||)$ est un espace vectoriel normé euclidien, on note $\langle ., \rangle$ son produit scalaire. Soit G un sous groupe compact de $GL(E)$. Alors il existe $u \in GL(E)$ tel que $u^{-1}Gu$ soit un sous-groupe de $O(E)$.

14.6 Preuve

Proof of Lemma 14.5. H est compact donc pour tout $x \in V$, l'application continue $h \mapsto ||h(x)||$ y admet un maximum en un certain h_x. Posons alors

$$N : \left\{ \begin{array}{ccc} V & \to & \mathbb{R}^+ \\ x & \mapsto & \sup_{u \in H} ||u(x)|| \end{array} \right.$$

— N définit bien une norme sur V.
— Cette norme est invariante par H puisque H est un groupe.
— Cette norme est strictement convexe : Si $x \neq y$ alors par stricte convexité de $||.||$ il vient

$$\begin{aligned} N\left(\frac{x+y}{2}\right) &= \left\| \frac{h_{(x+y)/2}(x) + h_{(x+y)/2}(y)}{2}) \right\| \\ &< \frac{\|h_{(x+y)/2}(x)\| + \|h_{(x+y)/2}(y)\|}{2} \\ &\leq \frac{N(x) + N(y)}{2} \end{aligned}$$

Par continuité sur le compact K, N admet un minimum sur K, et par stricte convexité ce minimum est unique. Notons le a. Alors si $u \in H$,

$$N(u(a)) = \sup_{v \in H} \|v \circ u(a)\| = \sup_{w \in H} \|w(a)\| \leq N(a)$$

Or, K est laissé stable par tous les éléments de H, donc en particulier $u(a) \in K$. Puisque $N(a)$ est un minimum de N, on en déduit que $N(u(a))$ est aussi un minimum de N sur K et par unicité $u(a) = a$. □

Proof of Theorem 14.6.

Compte tenu de la remarque (14.4), on va donc chercher un point fixe pour l'action par congruence de G sur $S(E)$ via le théorème du point fixe de Kakutani : Pour $g \in G$ et $u \in S(E)$, on pose
Soit

$$\varphi : \left\{ \begin{array}{rcl} GL(E) & \to & GL(S(E)) \\ u & \mapsto & (v \mapsto u \circ v \circ u^*) \end{array} \right.$$

le morphisme définissant l'action. φ est continu, et par suite $H := \varphi(G)$ est un sous groupe compact de $GL(S(E))$.

$S^{++}(E)$ est un convexe non vide de $S(E)$, stable par l'action de G (donc stable par H). Cependant, il n'est pas compact, et on ne peut pas utiliser le théorème du point fixe de Kakutani. Considérons alors $C := \{v \circ v^* \mid v \in G\}$ l'orbite de l'identité. C'est bien une partie compacte. Soit K son enveloppe convexe. Par le théorème de Carathéodory, c'est encore une partie compacte de $S(E)$, contenue dans $S^{++}(E)$ puisqu'il est convexe.

L'action de G étant affine, elle préserve les enveloppes convexes, et donc K est encore stable par H.

Par le théorème de *Kakutani* 14.5, il existe $w \in K \subset S^{++}(E)$ fixé par tous les éléments de H.

Soit $u \in S^{++}(E)$ la racine carrée de w. Alors, $w = u^2 = u \circ u^*$. Par suite, pour tout $g \in G, g \circ u \circ u^* \circ g^* = u \circ u^*$ et donc $u^{-1} \circ g \circ u \circ u^* \circ g^* \circ (u^{-1})^* = Id_E$ ie

$$(u^{-1} \circ g \circ u) \circ (u^{-1} \circ g \circ u)^* = Id_E$$

Par suite, $u^{-1} \circ g \circ u \in O(E)$ pour tout $g \in G$, et donc $u^{-1}Gu$ est un sous groupe de $O(E)$. □

15 Méthode de Laplace [Timé]

15.1 Remarques sur le timing

— Colonne 1 on écrit le dev + le dessin de φ. Faut finir en 2/3 min max.
— Colonne 2 on traite le cas de la gaussienne.
— Colonne 3 Le cas général, et on peut finir là.

Timing : 15'40 (un peu long, raccourcir l'exemple au début) mais sinon c'est un bon dev.

15.2 Recasages :

— 224 - Exemples de développements asymptotiques de suites et de fonctions.
— 228 - Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.
— 236 - Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.
— 239 - Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

15.3 Références :

— Rouvière [Rou03]

15.4 Prérequis

Savoir calculer l'intégrale de Gauss (par exemple changement de variables en polaire) :

$$\int_0^\infty e^{-x^2} dx = \frac{\sqrt{\pi}}{2} \tag{4.16}$$

15.5 Développement

Soit $a < b \leq +\infty$ et on considère $I = [a, b[$ un intervalle de $\mathbb{R} \cup \{+\infty\}$, $\phi : I \to \mathbb{R}$ de classe $\mathcal{C}^2$ et $f : I \to \mathbb{C}$ telle que $x \mapsto e^{-t_0\phi(x)} f(x)$ soit intégrable sur I pour un certain réel t_0.

On suppose de plus que f est continue en a et vérifie $f(a) \neq 0$.

L'objectif de ce développement est d'étudier le comportement lorsque $t \to \infty$ des fonctions F de la forme suivante :

$$F(t) := \int_I e^{-t\phi(x)} f(x) dx$$

Theorem 15.1. Si $\phi' > 0$ sur $]a, b[$, $\phi'(a) = 0$, $\phi''(a) > 0$:

$$F(t) \sim \sqrt{\frac{\pi}{2\phi''(a)}} e^{-t\phi(a)} f(a) \frac{1}{\sqrt{t}}$$

On propose de plus une application : Preuve de la formule de Stirling via la fonction Γ.

15.6 Preuve

Remarque préliminaire (à préciser à l'oral durant le développement, c'est pédagogique) Le terme exponentiel écrase tout lorsque son argument tend vers l'infini. La contribution majoritaire devrait donc se faire lorsque ϕ atteint un minimum sur I. Les hypothèses du théorème sont donc tout à fait raisonables.

Démonstration. Réalisons un développement de Taylor de ϕ autour de a :

$$\phi(x) = \phi(a) + 0 + \frac{1}{2}\phi''(a)(x-a)^2 + o((x-a)^2)$$

On a donc un terme en $e^{-t\phi(a)}$ et un terme quadratique qu'on va commencer par étudier comme cas particulier. Pour simplifier encore, étudions le cas d'une gaussienne $a = 0$ et $\phi(x) = x^2$:

Cas d'une Gaussienne La remarque préliminaire invite à découper l'intégrale autour de 0.

Puisque f est continue en 0 elle est bornée dans un voisinage de l'origine : il existe $\eta > 0$ et $M > 0$ tels que

$$\forall x \in I,\ |x| \leq \eta \Rightarrow |f(x)| \leq M$$

Par un changement de variable on a alors :

$$\int_0^\eta e^{-tx^2} f(x)dx = \frac{1}{\sqrt{t}} \int_0^{\sqrt{t}\eta} e^{-u^2} f\left(\frac{u}{\sqrt{t}}\right) du$$

Or,

$$\left| e^{-u^2} f\left(\frac{u}{\sqrt{t}}\right) \mathbb{1}_{[0,\sqrt{t}\eta]} \right| \leq M e^{-u^2}$$

qui est intégrable.

Par le théorème de convergence dominée, on déduit alors

$$\int_0^{\eta\sqrt{t}} e^{-u^2} f\left(\frac{u}{\sqrt{t}}\right) du \to \int_0^\infty e^{-u^2} f(0) du$$

Puisque $f(0) \neq 0$, en utilisant la valeur de l'intégrale de Gauss (4.16), on a donc :

$$\int_0^\eta e^{-tx^2} f(x)dx \underset{t\to\infty}{\sim} \frac{f(0)}{2}\sqrt{\frac{\pi}{t}}$$

D'autre part pout $t \geq t_0$,

$$\left|\int_\eta^b e^{-tx^2} f(x)dx\right| \leq e^{-(t-t_0)\eta^2} \int_\eta^b e^{-t_0x^2} |f(x)|\, dx$$
$$\to 0$$

Finalement :

$$\int_0^b e^{-tx^2} f(x)dx \underset{t\to\infty}{\sim} \frac{f(0)}{2}\sqrt{\frac{\pi}{t}}$$

Retour au cas général Compte-tenu du développement limité de ϕ, pour se ramener au cas particulier on fait le changement de variable $\phi(x) = \phi(a) + y^2$:

L'application $x \overset{y}{\mapsto} \sqrt{\phi(x) - \phi(a)}$ est de classe $\mathcal{C}^1$ sur $]a, b[$ par composition et

$$y'(x) = \frac{\phi'(x)}{2\sqrt{\phi(x) - \phi(a)}} > 0$$

Par ailleurs au voisinage de a,

$$\phi'(x) = 0 + \phi''(a)(x-a) + o(x-a)$$
$$\phi(x) - \phi(a) = 0 + \frac{1}{2}\phi''(a)(x-a)^2 + o((x-a)^2)$$

Donc,

$$y'(x) = \frac{\phi''(a)(x-a) + o(x-a)}{\sqrt{2}(x-a)\sqrt{\phi''(a) + o((x-a))}}$$
$$\underset{x\to a}{\sim} \sqrt{\frac{\phi''(a)}{2}} > 0$$

Donc par le théorème de la limite de la dérivée, y est de classe $\mathcal{C}^1$ sur I, et $y' > 0$ sur I. Donc y réalise un $\mathcal{C}^1$-difféomorphisme de I sur un intervalle $[0, c[$ et le changement de variable est licite.

Soit $x = \psi(y)$ l'application réciproque. On a alors :

$$F(t) = e^{-t\phi(a)} \int_a^b e^{-ty(x)^2} f(x)dx$$
$$= e^{-t\phi(a)} \int_0^c e^{-ty^2} f(\psi(y))\psi'(y)dy$$

Comme $\psi' \times f \circ \psi$ est continue en 0, et

$$f(\psi(0))\psi'(0) = f(a)\sqrt{\frac{2}{\phi''(a)}} \neq 0$$

on peut appliquer le résultat prouvé dans le cas particulier :

$$F(t) \underset{t\to\infty}{\sim} \frac{1}{\sqrt{t}} e^{-t\phi(a)} f(a)\sqrt{\frac{\pi}{2\phi''(a)}}$$

□

Application à la fonction Γ : Formule de Stirling

$$\Gamma(t+1) = \int_0^\infty x^t e^{-x} dx = \int_0^\infty \exp\left(-[x - t\ln(x)]\right) dx$$

En étudiant la fonction $x \mapsto -x - t\ln(x)$ on voit qu'elle est strictement convexe, avec un minimum en t.

Pour se ramener à un minimum en 0 indépendant de t, on fait le changement de variable $x = t(u+1)$, alors $dx = tdu$ et

$$\Gamma(t+1) = t^{t+1} \int_{-1}^\infty e^{-t\phi(u)} du$$

avec $\phi(u) = 1 + u - \ln(1+u)$
ϕ est de classe $\mathcal{C}^2$ sur $]-1, 0]$ et $[0, \infty[$;

$$\phi'(u) = 1 - \frac{1}{1+u}$$
$$\phi''(u) = \frac{1}{(1+u)^2}$$

On applique deux fois le théorème précédent avec $f(0) = 1$, $\phi(0) = \phi''(0) = 1$ et en faisant le changement de variable u en $-u$ dans la seconde intégrale :

$$\int_0^\infty e^{-t\phi(u)} du = \sqrt{\frac{\pi}{2t}} + o\left(\frac{e^{-t}}{\sqrt{t}}\right)$$
$$\int_{-1}^0 e^{-t\phi(u)} du = \int_0^1 e^{-t\phi(-u)} du$$
$$= \sqrt{\frac{\pi}{2t}} + o\left(\frac{e^{-t}}{\sqrt{t}}\right)$$

D'où :

$$\Gamma(t+1) = \sqrt{2\pi\, t} e^{-t} t^t$$

On retrouve donc la formule de stirling :

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

16 Stabilité d'un système différentiel : Théorème de Liapounov

16.1 Références

— Rouvière [Rou03]

— Berthelin [Ber17]

16.2 Recasages :

— 220 - Équations différentielles $X' = f(t, X)$. Exemples d'étude des solutions en dimension 1 et 2.

— 221 - Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

16.3 Contexte

On considère un système différentiel autonome $Y' = f(Y)$. Sous des conditions raisonnables, les hypothèses du théorème de Cauchy-Lipschitz sont vérifiées et pour toute condition initiale, ce système admet une unique solution maximale.

Lorsque le système est linéaire, l'étude de l'exponentielle d'une matrice permet d'avoir des informations très précises sur le comportement de toutes les solutions. Mais dans la vraie vie, les trucs ne sont linéaires que dans pour des petites variations autour d'une position d'équilibre stable. Le théorème de Liapounov permet de préciser cela en exportant le cas linéaire vers le cas non linéaire.

16.4 Prérequis

Ce développement est long. Il ne faut pas hésiter à aller très vite sur certains points, mais il ne faut pas que ça nuise à la clarté de la présentation. Suivant la leçon peut-être ne donner que les idées du cas linéaire, en plaçant des mots clefs comme décomposition de Dunford ; ou bien aller vite sur les calculs dans le cas non linéaire. Dans tous les cas, il faut s'entraîner.

16.5 Développement

On commence par voir ce qu'il se passe dans le cas linéaire, avant d'en déduire le cas non linéaire. Si ce développement a évidemment toute sa place dans la leçon 220, à mon sens c'est aussi vrai pour la leçon sur les équa diff linéaires 221 puisque l'on étudie d'abord le cas d'un système linéaire et que c'est bien cette étude qui donne l'intuition du résultat dans le cas non linéaire.

Theorem 16.1. Soit A dans $\mathcal{M}_n(\mathbb{C})$. On suppose que les valeurs propres de A sont de partie réelle strictement négative. Alors toutes les solutions du système différentiel linéaire $Y' = AY$ tendent exponentiellement vite vers 0 lorsque $t \to \infty$.

Theorem 16.2. Soit $f : \mathbb{R}^n \to \mathbb{R}^n$ une application de classe $\mathcal{C}^1$ telle que $f(0) = 0$. Soit $A = df(0)$ la matrice linéarisée de f. On suppose que les valeurs propres de A sont de partie réelle strictement négative. Alors pour tout x suffisament proche de 0, la solution maximale de

$$\begin{cases} y' &= f(y) \\ y(0) &= x \end{cases}$$

tend exponentiellement vite vers 0 lorsque $t \to \infty$.

16.6 Preuve

Proof of Theorem 16.1. Fixons x. Par le théorème de Cauchy Lipschitz linéaire, $y' = Ay'$ admet une unique solution globale définie sur $\mathbb{R}$, vérifiant la condition initiale $y(0) = x$. Elle est donnée par

$$y(t) = e^{tA}x$$

.

Ignorer ce qui suit, reprendre au prochain encadré, on va gagner du temps avec Dunford

Soit $\lambda_1, \dots, \lambda_k$ les valeurs propres distinctes de A. On note m_j la multiplicité de λ_j. On décompose $\mathbb{C}^n$ selon les espaces caractéristiques $E_j = \ker(A - \lambda_j I)^{m_j}$

$$\mathbb{C}^n = \bigoplus_{j=1}^{k} E_j$$

et soit $x = x_1 + \cdots + x_k$ la décomposition de x selon cette somme directe.

Chaque E_j est stable par A et sur E_j,

$$e^{tA}x_j = e^{t\lambda_j}(e^{t(A-\lambda_j I)}x_j) = e^{t\lambda_j}\left(\sum_{p=0}^{m_j-1}\frac{t^p}{p!}(A-\lambda_j I)^p\right)x_j$$

Alors pour une norme sur $\mathbb{C}^n$ il vient

$$\begin{aligned}\|e^{tA}x_j\| &\leq |e^{t\lambda_j}|\sum_{p=0}^{m_j-1}\frac{|t|^p}{p!}\|A-\lambda_j I\|^p\|x_j\| \\ &\leq e^{t\Re(\lambda_j)}C_j\left(\sum_{p=0}^{m_j-1}\frac{|t|^p}{p!}\right)\|x_j\| \\ &\leq e^{t\Re(\lambda_j)}C_j\left(1+|t|\right)^{m_j-1}\|x_j\|\end{aligned}$$

Où l'on a utilisé le binôme de Newton, et C_j est une constante dépendant de j.

Par suite,

$$\begin{aligned}\|e^{tA}\| &\leq \sum_{j=1}^{n} \|e^{tA}x_j\| \\ &\leq \sum_{j=1}^{n} e^{t\Re(\lambda_j)} C_j \left(1+|t|\right)^{m_j-1} \|x_j\| \\ &\leq C\|x\|(1+|t|)^{n-1} \sum_{j=1}^{n} e^{t\Re\lambda_j}\end{aligned}$$

Or, par hypothèse il existe $a > 0$ tel que pour tout j, $\Re(\lambda_j) < -a$. Dès lors, $(1+|t|)^{n-1}e^{t\Re(\lambda_j)}e^{ta}$ est bornée par une constante C'. Par suite, il existe M tel que

$$\|y(t)\| \leq Me^{-ta}\|x\|$$

On commence ici

On a $y(t) = e^{tA}x$. Soit $A = D + N$ la décomposition de Dunford de A. On note d l'indice de Nilpotence de N. Alors $e^{tA} = e^{tD}e^{tN}$. Soit $\|.\|$ une norme matricielle. Alors :

$$\|e^{tA}\| \leq \|e^{tD}\|\|e^{tN}\|$$

Or,

$$\|e^{tN}\| \leq \sum_{k=0}^{d} \frac{|t|^k}{k!}\|N\|^k \leq C_N|t|^d$$

D'autre part, $e^{tD} = Pe^{t\Delta}P^{-1}$ avec Δ diagonale. Par sous multiplicativité :

$$\|e^{tD}\| \leq \|P\|\|P^{-1}\|\|e^{t\Delta}\|$$

Prenons alors la norme $\|\cdot\|$ subordonnée à la norme $\|\cdot\|_\infty$ de sorte que

$$\|e^{t\Delta}\| = \max_{\lambda\in Sp(A)} |e^{t\lambda}| = \max_{\lambda\in Sp(A)} e^{\Re(t\lambda)} = e^{\Re(t\lambda_0)}$$

Par suite,

$$\|e^{tA}\| \leq Ce^{\Re(t\lambda_0)}|t|^n$$

Or, par hypothèse il existe $a > 0$ tel que pour tout λ, $\Re(\lambda) < -a$. Dès lors, $|t|^n e^{t\Re(\lambda)}e^{ta}$ est bornée par une constante C'. Par suite, il existe M tel que

$$\|e^{tA}\| \leq Me^{-ta}$$

d'où

$$\|y(t)\| \leq Me^{-ta}\|x\|$$

□

Proof of Theorem 16.2. Fixons $x \in \mathbb{R}^n$. f est $\mathcal{C}^1$ donc par le théorème de Cauchy-Lipschitz, le problème de Cauchy

$$\begin{cases} y' &= f(y) \\ y(0) &= x \end{cases}$$

admet une unique solution maximale (y, I) avec $0 \in I$.

L'idée pour obtenir le comportement de y va être de linéariser le système, et, en s'appuyant sur le système linéaire, d'obtenir une inéquation différentielle vérifiée par y pour conclure via un résultat à la Gronwall.

Linéarisation du système Par un développement limité autour de 0, $f(y) = f(0) + Ay + r(y) = Ay + r(y)$ où $r(y) = o(\|y\|)$. Par suite, le système différentiel se réécrit de la façon suivante :

$$\begin{cases} y' &= Ay + r(y) \\ y(0) &= x \end{cases}$$

Changement de norme En utilisant l'intuition du système linéaire, pour $x, y \in \mathbb{R}^n$ on pose $\varphi_{x,y}(t) := \langle e^{tA}x \mid e^{tA}y\rangle$. Alors, par l'inégalité de Cauhcy-Schwarz, et la majoration précédente on en déduit

$$\begin{aligned} |\varphi_{x,y}(t)| &\leq \|e^{tA}x\|\|e^{tA}y\| \\ &\leq M^2 e^{-2ta}\|x\|\|y\| \end{aligned}$$

Par suite, pour tout $x, y \in \mathbb{R}^n$, $\varphi_{x,y}$ est intégrable sur $\mathbb{R}^+$. Introduisons alors la forme bilinéaire symétrique suivante

$$b(x, y) := \int_0^\infty \varphi_{x,y}(t)dt$$

$b(x, x) = \displaystyle\int_0^\infty \|e^{tA}x\|^2 dt$ donc b définit un produit scalaire. On note q la forme quadratique associée de sorte que $\sqrt{q}$ soit une norme sur $\mathbb{R}^n$, donc équivalente à la norme euclidienne.

Inéquation différentielle Par composition, $q(y)$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}$ et $q(y)' = dq(y)y'$

Or, par dérivation d'une forme quadratique sur $\mathbb{R}^n$, $dq(y) = h \mapsto 2b(y, h)$.

Par suite,

$$q(y)' = 2b(y, y')$$

Or, $y' = Ay + r(y)$, d'où

$$q(y)' = 2b(y, Ay) + 2b(y, r(y))$$

.

— D'une part

$$\begin{aligned} 2b(y, Ay) &= \int_0^\infty 2\langle e^{tA}y \mid e^{tA}Ay\rangle dt \\ &= \lim_{T\to\infty} \int_0^T \left(\|e^{tA}y\|^2\right)' dt \\ &= \lim_{T\to\infty} \left[\|e^{tA}y\|^2\right] \\ &= -\|y\|^2 \end{aligned}$$

— D'autre part, en utilisant l'inégalité de Cauchy-Schwarz il vient

$$b(y, r(y)) \leq \sqrt{q(y)}\sqrt{q(r(y))}$$

Or, $r(y) = o(\|y\|)$ donc pour tout $\varepsilon > 0$ il existe $\alpha > 0$ tel que

$$q(y) < \alpha \Rightarrow \sqrt{q(r(y))} < \varepsilon\sqrt{q(y)}$$

et donc

$$b(y, r(y)) \leq \varepsilon q(y)$$

pour $q(y) < \alpha$.

On en déduit que si $q(y) < \alpha$ alors

$$q(y)' \leq -\|y\|^2 + \varepsilon q(y)$$

.

Par équivalence des normes en dimension finie, il existe C telle que $\|y\|^2 \geq Cq(y)$ et donc

$$q(y) < \alpha \Rightarrow q(y)' \leq -\beta q(y)$$

où $\beta = C - 2\varepsilon > 0$ pour ε assez petit.

En appliquant le théorème des bouts on vérifie simplement que si $q(x) < \alpha$ alors $\mathbb{R}^+ \subset I$ et que cette inéquation est valide sur tout $\mathbb{R}^+$. On peut alors conclure que

$$q(y)(t) \leq Me^{-\beta t}q(x)$$

16.7 Post requis : Fin de la preuve

L'inéquation est valide partout Supposons que x a été choisi de sorte que $q(x) < \alpha$. Si $q(y)$ n'est pas bornée par α sur $\mathbb{R}^+$ alors soit $t_0 := \min\{t \mid q(y)(t) = \alpha\}$. C'est un fermé non vide, donc t_0 existe bien et $q(t_0) = \alpha$.

$q(y)$ est continue sur $[0, t_0]$, dérivable sur $]0, t_0[$ et par hypothèse $q(y)'(t) < 0$. Donc $q(y)$ y est décroissante et donc $x = q(0) \leq q(t_0)$. Or $q(t_0) = \alpha$ et $q(x) < \alpha$. Absurde.

Donc $q(y)$ est bornée à droite sur son intervalle de définition. Par le théorème des bouts on en déduit que $[0, \infty[\subset I$ d'une part, et d'autre part que l'inéquation différentielle est valide sur $\mathbb{R}^+$. □

17 Théorème de Lie-Kolchin [Timé]

17.1 Remarques sur le timing

— Dev juste parfait, attention aux labsus, mais il time très bien. Il faut être au clair sur les notions de groupe dérivé & co.

— Colonne 1 on fait le cas du groupe abélien, on énonce la propriété absurde, on donne la stabilité de P par G, donc de V. On insiste bien.

— Colonne 2 on fini cette partie 1.

— Colonne 3 passage au quotient et induit.

— Colonne 4 Récurrence.

Timing : 15' c'est parfait.

17.2 Recasages :

— 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de $GL(E)$. Applications.

— 157 - Endomorphismes trigonalisables. Endomorphismes nilpotents.

17.3 Référence :

Algèbre Corporelle, Chambert-loir [CL05]

17.4 Contexte

Je mets ici quelques rappels sur les groupes dérivés et résolubles. Il ne sont pas utiles stricto-sensus au développement, mais il est bon d'avoir ces résultats en tête le jour de l'oral.

Definition 17.1. Soit G un groupe. On dit qu'il est résoluble s'il existe $k \in \mathbb{N}$ et une suite de sous-groupes distingués

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$$

tel que pour tout i, le quotient G_i/G_{i+1} soit commutatif. Le n minimal sera appelé classe de résolubilité de G.

La notion de groupe résoluble se comporte très bien vis à vis des sous-groupes et des quotients dans le sens suivant :

Theorem 17.2. Soit G un groupe et H un sous-groupe de G. Alors

(i) Si G est résoluble alors H est résoluble.

(ii) Si G est résoluble et H est distingué dans G alors G/H est résoluble.

(iii) Si H est résoluble et distingué, et si G/H est résoluble alors G est résoluble.

Démonstration.

(i) Soit (G_i) une suite de sous-groupes donnée par la résolubilité de G et posons $H_i := H \cap G_i$. Alors la restriction à H_{i+1} du morphisme de projection

$$\pi_i : G_{i+1} \to G_{i+1}/G_i$$

a pour noyau $G_i \cap H_{i+1} = G_i \cap (G_{i+1} \cap H) = G_i \cap H = H_i$. En particulier $H_i \lhd H_{i+1}$ et par le théorème d'isomorphisme, $H_{i+1}/H_i \simeq G_{i+1}/G_i$ est donc abélien. Par suite H est résoluble.

(ii) Soit $\pi : G \to G/H$ la surjection canonique. G est résoluble, donc comme précédemment considérons G_i une suite distinguée et posons $K_i := \pi(G_i)$. Alors K_i est une suite de sous-groupes de G/H. Par ailleurs, si $g = \pi(g_{i+1}) \in K_{i+1}, h = \pi(h_i) \in K_i$ alors $ghg^{-1} = \pi(g_{i+1}h_ig_{i+1}^{-1}) \in K_i$ puisque $G_i \lhd G_{i+1}$. Donc $K_i \lhd K_{i+1}$. De plus, le morphisme $G_{i+1} \to K_{i+1} \to K_{i+1}/K_i$ est surjectif comme composée de deux morphismes surjectifs, et son noyau contient G_i. Par suite, il se factorise en un morphisme surjectif $G_{i+1}/G_i \to K_{i+1}/K_i$. Comme G_{i+1}/G_i est abélien, on en déduit que K_{i+1}/K_i est aussi abélien. Par suite, G/H est bien résoluble.

(iii) Soit $\{1\} = H_0 \lhd \cdots \lhd H_n = H$ et $\{\bar{1}\} = K_0 \lhd \cdots \lhd K_m = G/H$ deux suites distinguées telles que H_{i+1}/H_i et K_{i+1}/K_i soient abéliens. Soit $\pi : G \to G/H$ la surjection canonique. Alors $H = Ker\pi = \pi^{-1}(K_0)$. Posons

$$G_i := \begin{cases} H_i & \text{si } i \leq n \\ \pi^{-1}(K_{i-n}) & \text{si } i \geq n \end{cases}$$

Alors (G_i) est une suite de sous groupes de G. Vérifions qu'elle est distinguée. C'est évident pour $i < n$. Soit $i \geq n$. Le morphisme

$$G_{i+1} = \pi^{-1}(K_{i+1-n}) \xrightarrow{\pi} K_{i+1-n} \to K_{i+1-n}/K_{i-n}$$

est surjectif, de noyau $\pi^{-1}(K_{i-n}) = G_i$. Par conséquent $G_i \lhd G_{i+1}$ d'une part, et d'autre part ce morphisme se factorise en un isomorphisme

$$G_{i+1}/G_i \simeq K_{i+1-n}/K_{i-n}.$$

Finalement, on a bien une suite distinguée

$$\{1\} = G_0 \lhd \cdots \lhd G_n = H_n = \pi^{-1}(K_0) \lhd \cdots \lhd G_{n+m} := \pi^{-1}(K_m) = G$$

tel que G_{i+1}/G_i est abélien. Donc G est bien résoluble. □

Theorem 17.3. Soit G un groupe. On note $D^n(G) := D(D^{n-1}(G))$ la suite itérée des groupes dérivés de G. Alors :

$$G \text{ est résoluble } \Leftrightarrow \exists n \in \mathbb{N}\ D^n(G) = \{1\}$$

Démonstration.

$\Rightarrow$ On fait la preuve sur la classe de résolubilité.

— $n = 0$ ssi G est trivial.

— Si G est résoluble de classe n, considérons une suite distinguée

$$\{1\} =: G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

. Alors G_{n-1} est résoluble de classe $n-1$, donc par hypothèse de récurrence, $D^{(n-1)}(G_{n-1}) = \{1\}$. Or, G/G_{n-1} est abélien, donc $D(G) \subset G_{n-1}$. Par suite,

$$D^n(G) \subset D^{(n-1)}(G_{n-1}) = \{1\}.$$

D'où le résultat.

$\Leftarrow$ Soit n tel que $D^{(n)}(G) = \{1\}$. Alors

$$\{1\} = D^{(n)}(G) \lhd D^{(n-1}(G) \lhd \cdots \lhd D(G) \lhd G$$

et $D^i(G)/D^{(i+1)}(G)$ est abélien. Donc G est résoluble, de classe au plus n.

□

Exemples :

— Les groupes résolubles de classe ≤ 1 sont les groupes abéliens

— Tout sous groupe d'un groupe résoluble est résoluble

— Un groupe simple est résoluble ssi il est abélien (car $D(G) \lhd G$) ssi c'est $\mathbb{Z}/p\mathbb{Z}$ pour p premier.

— Le groupe fini non résoluble de plus petit cardinal est A_5 d'ordre 60.

— Pour $n \geq 5$ A_n est simple et non abélien, donc non résoluble.

— S_n est résoluble ssi $n \leq 4$.

— Pour le folklore on énonce le théorème suivant dit de Feit-Thompson (aussi connu sous le nom théorème de l'ordre impair), et qui a été prouvé en Coq par Gonthier et al. [GAA+13].

> **Theorem 17.4** (Feit-Thompson)**.** Tout groupe fini d'ordre impair est résoluble.

17.5 Prérequis

Il faut évidemment être au clair sur la notion de groupe dérivé, résoluble et tutti quanti, et avoir des idées sur ce que ça peut évoquer dans la tête du Jury :

— Groupe nilpotent

— Résolubilité par radicaux

— Théorie de Galois

mais la réponse "Je ne sais pas" est bien entendu acceptable !

Lemma 17.5. Toute famille de matrices qui commutent deux à deux est co-trigonalisable. En particulier, tout sous-groupe abélien de $GL_n(\mathbb{C})$ est co-trigonalisable.

Theorem 17.6. Soit G un groupe résoluble, et $\varphi : G \to H$ un morphisme de groupes. Alors $\Im(\varphi)$ est résoluble.

Démonstration. L'image d'un commutateur par un morphisme de groupes est un commutateur. Par suite, $\varphi(D(G)) = D(\varphi(G))$. Supposons G résoluble de classe n. Alors

$$D^n(\varphi(G)) = \varphi(D^n(G)) = \varphi(\{e\}) = \{e\}.$$

Par suite, $\varphi(G)$ est résoluble, de classe au plus n. □

Theorem 17.7. Soit G un sous-groupe connexe de $GL_n(\mathbb{C})$. Alors son sous-groupe dérivé est connexe.

Démonstration. L'ensemble S de tous les commutateurs est l'image de $G \times G$ par l'application continue $(x, y) \mapsto xyx^{-1}y^{-1}$. Donc S est connexe. De plus, l'inverse d'un commutateur est encore un commutateur. Donc $I_n \in S$. Pour tout $m \geq 1$ notons S_m l'ensemble des produits à m facteurs d'éléments de S. Par la même remarque sur l'inverse on en déduit que

$$D(G) = \cup_{m \geq 1} S_m.$$

Or, S_m est l'image de S^m par l'application continue $(g_1, \ldots, g_m) \mapsto g_1 \ldots g_m$. Comme S est connexe il en est de même pour S^m et par suite S_m est aussi connexe. $D(G)$ est donc connexe comme union d'ensembles connexes ayant au-moins un point en commun (l'identité). □

17.6 Développement

Theorem 17.8 (Lie-Kolchin)**.** Tout sous-groupe connexe résoluble de $GL_n(\mathbb{C})$ est co-trigonalisable

Démonstration. On va raisonner par récurrence sur la dimension n.

— Si $n = 1$ c'est évident, toutes les matrices sont triangulaires supérieures.

— Supposons le résultat vrai pour $1 \leq m < n$. Soit G un sous-groupe connexe et résoluble de $GL_n(\mathbb{C})$. On va alors raisonner en deux temps.

1ère étape : Il existe un sev strict de $\mathbb{C}^n$ stable par G

Par l'absurde supposons que les seuls sev stables par G sont triviaux, et faisons une disjonction de cas selon que G est abélien ou non :

— Si G est abélien. Par le lemme 17.5, G est cotrigonalisable, et donc il existe une droite stable par tous les éléments de G. On en déduit que $n = 1$. Absurde.

— Sinon, G est résoluble de classe $k \geq 2$ et on pose $H := D^{k-1}(G)$. C'est un groupe abélien non trivial. Notons P l'ensemble des vecteurs propres communs à tous les éléments de H. Comme il est abélien $P \neq \emptyset$. Posons $V := Vect(P)$ et vérifions qu'il est stable par G. Par linéarité, il suffit de vérifier la stabilité sur les éléments de P. Soit $g \in G$, $v \in P$ et $h \in H$. Alors

$$h(g(v)) = gg^{-1}hg(v) = g(g^{-1}hg)(v)$$

Or, $H \lhd G$ donc $g^{-1}hg \in H$ et par suite v est un vecteur propre de $g^{-1}hg$. Ainsi, $g(v)$ est encore un vecteur propre de h et ainsi V est stable par G.
Comme $V \neq \{0\}$ on en déduit que $V = \mathbb{C}^n$ ie que $\mathbb{C}^n$ possède une base de vecteurs propres communs à tous les éléments de H, ie H est codiagonalisable. Quitte à effectuer un changement de base, on peut supposer que les matrices de H sont toutes diagonales.
Faisons agir G sur H par conjugaison et fixons $h \in H$. L'action étant continue, l'orbite de h est connexe. Or, elles est formée de matrices diagonales, avec les mêmes valeurs propres qur h. Elle est donc finie. Or, une partie connexe et finie de $GL_n(\mathbb{C})$ a au plus un élément. On en déduit que l'orbite de h est réduite au singleton $\{h\}$. Par suite, $H \subset Z(G)$.
Soit $h \in H$ et W un espace propre de h. Comme h commute avec tous les éléments de G, W est stable par G. Par suite, $W = \mathbb{C}^n$ et h est scalaire : Il existe $\lambda_h \in \mathbb{C}$ tel que $h = \lambda_h I_n$. Or, le déterminant d'un commutateur vaut 1 donc puisque $k > 1$, $H \subset SL_n(\mathbb{C})$. Par suite, λ_h est une racine $n-$ième de l'unité. On en déduit que H est un groupe fini.
Or, par le théorème 17.7 H est connexe. Comme il est fini il est réduit à $\{I_n\}$. Absurde.

On considèrera donc dans la suite V un sev non trivial stable par G et on note m sa dimension avec $1 \leq m < n$.

2ème étape : On peut maintenant faire la récurrence

Soit W un supplémentaire de V. Puisque V est stable, dans une base adaptée à la décomposition $\mathbb{C}^n = V \oplus W$, les matrices de G sont toutes de la forme

$$\begin{pmatrix} g_V & u \\ 0 & g_W \end{pmatrix}$$

— Considérons le morphisme de groupes

$$\varphi_V : \left\{ \begin{array}{ccc} G & \to & GL_m(\mathbb{C}) \\ g & \to & g_V \end{array} \right.$$

φ est continue, donc $Im(\varphi)$ est un sous-groupe connexe de $GL_m(\mathbb{C})$. De plus $Im(\varphi)$ est résoluble comme image d'un groupe résoluble par un morphisme de groupes. Par l'hypothèse de récurrence, $Im(\varphi)$ est donc cotrigonalisable et on note B_V une base de trigonalisation commune.

— De même, on considère le morphisme de groupes

$$\varphi_W : \left\{ \begin{array}{ccc} G & \to & GL_{n-m}(\mathbb{C}) \\ g & \to & g_W \end{array} \right.$$

Son image est encore un sous-groupe connexe et résoluble. Par l'hypothèse de récurrence W possède une base commune de cotrigonalisation B_W.

Alors la réunion $B_V \sqcup B_W$ est une base de $\mathbb{C}^n$ dans laquelle la matrice de tous les éléments de G est triangulaire supérieure.

□

18 Primalité des nombres de Mersenne [Timé]

18.1 Remarques sur le timing

— Dev long, il faut aller vite, mais il est très bien. Laisse plein de trucs en suspens, donc attention aux exos. Mais comme j'ai la réciprocité quadratique en dev, je suis chaud.

— Ne pas parler de Krull, laisser le Jury poser la question.

— Colonne 1 on a la réciprocité quadratique, + le lemme prouvé par récurrence (ne pas faire la preuve, elle est facile, laisser le jury la demander).

— Colonne 2 On pose l'extension, on prouve que 2 admet une racine carrée. Calcul de $\overline{\rho}\rho = -1$.

— Colonne 3 on conclut le sens direct et on introduit le sens indirect.

— On précise l'extension et ce que veut dire $\sqrt{3}$.

— Ne pas trop s'attarder sur la caractéristique de l'anneau, elle est claire. Quand on développe Q, c'est aussi clair qu'il est à coef dans le sous corps premier ($\overline{4} = 4 \times \overline{1}$).

— Morphisme de frobenius, racines et tutti quanti. Il faut aller vite sur la fin.

Timing : 18'++ mais cafouillage à la fin, revoir le dev. Ne pas faire la récurrence $2^{2n+1} - 1 \equiv 7 \mod 12$. Et accélerer sur les calculs éventuellement.

18.2 Recasages :

— 120 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

— 121 - Nombres premiers. Applications.

— 141 - Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications.

— 123 - Corps finis. Applications. ? ?

18.3 Références :

— *Calcul formel*, Picart, Rannou [SPR02]

18.4 Contexte

On appelle $q - ieme$ nombre de Mersenne le nombre $M_q := 2^q - 1$. On a le fait facile suivant

Theorem 18.1. Si M_q est premier, alors q est premier.

En revanche, la réciproque est fausse : $M_{11} = 2047 = 23 \times 89$. On va chercher à caractériser les nombres de Mersenne qui sont premiers.

A partir de maintenant, $\sqrt{3}$ va désigner une racine carrée de 3 dans une extension convenable de $\mathbb{Z}_{M_q}$ à préciser.

18.5 Développement

Theorem 18.2. Pour tout nombre premier impair q, on a

$$M_q \text{ premier } \Leftrightarrow (2+\sqrt{3})^{2^{q-1}} \equiv -1 \mod M_q$$

Démonstration.

Première implication $\Rightarrow$

Supposons que M_q est premier, de sorte que $k := \mathbb{Z}_{M_q}$ est un corps.

1ère étape : Caractérisation des carrés modulo p Soit p un nombre premier impair. Alors, d'après la loi de réciprocité quadratique (25),

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$$

donc

$$3 \text{ est un carré } \mod p \Longleftrightarrow \left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}$$

Or, le seul carré non nul dans $\mathbb{Z}/3\mathbb{Z}$ est 1. Ainsi, 3 est un carré modulo p ssi l'une des deux alternatives suivantes a lieu

1. $p \equiv 1 \mod 3$ et $p \equiv 1 \mod 4$
2. $p \equiv -1 \mod 3$ et $p \equiv 3 \mod 4$

Or, 1 équivaut à $p \equiv 1 \mod 12$ et 2 équivaut à $p \equiv -1 \mod 12$ (Théorème chinois)

2ème étape : On calcule $M_q \mod 12$ Par récurrence, on prouve que $2^{2n+1} - 1 \equiv 7 \mod 12$ pour tout entier n.

— Initialisation : $2^{2.1+1} - 1 = 7$

— Supposons que $2^{2n+1} - 1 \equiv 7 \mod 12$. Alors,

$$2^{2(n+1)+1} - 1 = 4.2^{2n+1} - 1 = 4.(2^{2n+1} - 1) + 3 \equiv 4 \times 7 + 3 \equiv 7 \mod 12$$

En particulier, pour tout q premier impair, $M_q \equiv 7 \not\equiv \pm 1 \mod 12$.

Par conséquent, 3 n'est pas un carré, et par suite le polynôme $X^2 - 3$ est irréductible dans $\mathbb{Z}/M_q\mathbb{Z}$. Posons $L := k[X]/\langle X^2 - 3\rangle$. C'est une extension de k qui possède une racine carrée de 3, qu'on note $\sqrt{3}$.

En revanche,

$$2(2^q - 1) \equiv 0 \mod M_q \Rightarrow 2^{q+1} \equiv 2 \mod M_q$$

donc

$$2^{\frac{q+1}{2}} \text{est une racine carrée de 2 } \textbf{dans k} \tag{4.17}$$

(et donc dans L). On la notera $\sqrt{2}$.

Soit enfin ρ une racine du polynôme $X^2 - (2+\sqrt{3})$ dans L définie par :

$$\rho := \frac{1+\sqrt{3}}{\sqrt{2}}.$$

On notera

$$\overline{\rho} := \frac{1-\sqrt{3}}{\sqrt{2}}.$$

Alors d'une part,

$$\rho\overline{\rho} = -1$$

et d'autre part

$$(2+\sqrt{3})^{2^{q-1}} = (2+\sqrt{3})^{\frac{M_q+1}{2}} = (\rho^2)^{\frac{M_q+1}{2}} = \rho^{M_q+1}$$

(Attention, $x^{1/2}$ n'a *a priori* pas de sens dans L, on ne manipule que des puissances entières).

Or, comme L est de caractéristique M_q,

$$(1+\sqrt{3})^{M_q} = 1+\sqrt{3}^{M_q} = 1+\sqrt{3}\times(\sqrt{3}^2)^{\frac{M_q-1}{2}} = 1+\sqrt{3}\times 3^{\frac{M_q-1}{2}} = 1+\sqrt{3}\left(\frac{3}{M_q}\right) = 1-\sqrt{3}$$

puisque 3 n'est pas un carré.

D'autre part on rappelle que $\sqrt{2} \in k$ (4.17), donc est fixé par le morphisme de Frobenius. En particulier, $\sqrt{2}^{M_q} = \sqrt{2}$ (dans L). Finalement, $\rho^{M_q} = \overline{\rho}$.

On en déduit que

$$(2+\sqrt{3})^{2^{q-1}} = \rho^{M_q+1} = \rho\overline{\rho} = -1$$

.

Réciproque $\Leftarrow$

On va encore se placer dans une extension dans laquelle 3 admet une racine carrée. Si 3 est déjà un carré modulo M_q, on prend simplement $L = \mathbb{Z}/M_q\mathbb{Z}$. Sinon, on prend $L = \mathbb{Z}_{M_q}[X]/\langle X^2-3\rangle$. Attention, ce n'est pas un corps a priori, mais c'est un anneau fini.

Raisonnons par l'absurde, en supposant M_q non premier et considérons p un de ses facteurs premiers. p est donc non inversible dans L. Il existe alors un idéal maximal $\mathcal{I} \neq L$ de L contenant p (On vit dans un anneau fini, donc ne pas invoquer Krull). L'anneau quotient $K = L/\mathcal{I}$ est alors un corps, de caractéristique p.

Soit α, β les classes de $2+\sqrt{3}$ et $2-\sqrt{3}$ dans K. Par hypothèse, $\alpha^{2^{q-1}} \equiv -1 \mod M_q$. Alors, puisque K n'est pas de caractéristique 2, on en déduit que α est d'ordre 2^q.

D'autre part, le polynôme $Q = (X-\alpha)(X-\beta)$ est un polynôme à coefficient dans le sous-corps premier de K, qui est isomorphe à $\mathbb{Z}/p\mathbb{Z}$. Par suite, comme α est racine de Q, alors α^p est aussi racine de Q. Deux cas sont possibles :

- Soit $\alpha^p = \alpha$, et alors 2^q divise $p-1$. Mais p divise $M_q = 2^q - 1$ donc $p < 2^q$. C'est absurde.
- Ou bien $\alpha^p = \beta = \alpha^{-1}$. Alors, de $1 = \alpha^{2^q} = \alpha^{M_q+1}$ on déduit que $\alpha^p = \alpha^{M_q}$. Alors nécessairement $p \equiv 2^q - 1 \mod 2^q$, ce qui impose $p = 2^q - 1 = M_q$. C'est absurde car M_q a été supposé non premier.

Conclusion : Par suite M_q est premier, d'où le résultat. □

19 Résolution de systèmes linéaires : Méthodes itératives [Timé]

19.1 Remarques sur le timing

— Faire attention, ce dev est facile, et semble très court (c'est pour ça que j'avais préparé un exemple) mais pas du tout.

— Le début est évidemment expéditif, mais la partie interessante sur la norme au milieu n'est vraiment pas si rapide que ça, surtout si on veut expliquer d'où sort la norme qu'on pose (on veut $\|A\| = \|T_\delta\|_\infty$ donc on pose la norme ad-hoc sur $\mathbb{C}^n$.

— Ne pas se tromper de sens sur la norme qu'on pose. Si jamais on s'est trompé, tant pis, on s'excuse et on la change. De toute façon on s'en rend compte très vite, et puisqu'on a expliqué ce qu'on souhaitait obtenir le jury ne va pas trop en tenir rigueur (enfin je pense).

— Pour les leçons sur les systèmes linéaires, on commence par présenter la mise sous forme de point fixe, et on introduit le vecteur d'erreur. On se ramène donc à étudier la convergence d'une suite.

— Pour la leçon suite récurrente, on peut faire comme pour les systèmes linéaires en vrai, ou alors commencer par le critère de convergence et faire l'application. On perd peut-être moins de temps à faire comme les systèmes linéaires ? Si on fait comme ça, on décale les colonnes de 1 vers la droite, et la colonne 1 sert à cette mise en point fixe (et à écrire les 4 équivalences).

— Colonne 1 on écrit les 4 équivalences *Dans l'ordre !!!, c'est important sinon on risque de se perdre ... Donc on prend son plan avec soi pour recopier le dev.* On aura aussi la place de faire $(i) \Rightarrow (ii) \Rightarrow (iii)$.

— Colonne 2 on fait $(iv) \Rightarrow (i)$ en haut. On marque une séparation pour dire que le cas intéressant c'est ce qu'on va faire à présent.

— Colonne 2 (suite) écrit la trigonalisation de A et on introduit δ. Pendant qu'on fait ça, à l'oral on parle du degré de liberté qu'on gagne en introduisant le ε. Et ça c'est cool !

— Colonne 3 on présente la norme subordonnée qu'on veut obtenir, on introduit la norme sur $\mathbb{C}^n$ et on fait le calcul pour vérifier qu'on a ce qu'on veut. Enfin on peut conclure.

— Si on on l'a pas encore fait, en colonne 4 on présente la mise sous forme de point fixe et on introduit le vecteur d'erreur.

— Si c'est déjà terminé, on n'oublie pas de conclure ! Surtout pour les leçons sur les systèmes linéaires. 30 secondes vont suffire, on revient sur le tableau où on a présenté la mise sous forme de point fixe et l'erreur.

Timing : 15'14 (en faisant le point fixe à la fin).

19.2 Recasages :

— 106 - Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupe de $GL(E)$. Applications.

— 156 - Exponentielle de matrices. Applications.

— 170 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

19.3 Références :

— Ciarlet [CL06]

— Rombaldi d'analyse Matricielle [Rom99]

19.4 Contexte

On considère un système linéaire linéaire $Ax = b$ de n équations à n inconnues avec $A \in GL_n(R)$. Il admet une unique solution, cependant l'inversion de A peut-être très coûteuse. L'idée est alors de construire une suite $(x^{(k)})_{k\in\mathbb{N}}$ d'éléments de $\mathbb{R}^n$ qui va converger ves la solution x du système, le calcul de chaque $x^{(k)}$ étant bien plus simple que la résolution directe du système.

Pour ce faire, on découpe $A = M - N$ avec M facilement inversible. Ainsi :

$$Ax = b \Leftrightarrow (M-N)x = b \Leftrightarrow x = M^{-1}(b + Nx)$$

et on est ramené à un problème de point fixe, qui se prête bien à une résolution itérative en posant

$$\left\{ \begin{array}{rcl} x_0 & = & b \\ x_{k+1} & = & M^{-1}(b + Nx_k) \end{array} \right.$$

Si cette suite converge, c'est nécessairement vers la solution de $Ax = b$. On s'intéresse donc naturellement aux conditions sous lesquelles la méthode est convergente, et au choix de la décomposition.

19.5 Développement

On note ρ le rayon spectral.

Theorem 19.1. Soit A dans $\mathcal{M}_n(\mathbb{C})$. Les conditions suivantes sont équivalentes :

(i) $\lim\limits_{k\to\infty} A^k = 0$

(ii) Pour toute valeur initiale x_0, la suite (x_k) définie par $x_{k+1} = Ax_k$ pour $k \geq 0$ converge vers 0.

(iii) $\rho(A) < 1$

(iv) Il existe au moins une norme matricielle induite telle que $\|A\| < 1$

Theorem 19.2. Soient $A = M - N$ une matrice inversible, avec M inversible. Alors la méthode itérative associée à la décomposition $A = M - N$ converge si et seulement si $\rho(M^{-1}N) < 1$.

19.6 Preuve

Proof of 19.1.

(i) ⇒ (ii) Résulte de

$$\|x_k\| = \|A^k x_0\| \leq \|A^k\| \|x_0\|$$

(ii) ⇒ (iii) Raisonnons par l'absurde, et supposons qu'il existe une valeur propre λ de A telle que $|\lambda| \geq 1$. Alors, si x_0 est un vecteur propre non nul associé à λ, en écrivant que $x_k = A^k x_0 = \lambda^k x_0$ il vient que la suite (x_k) ne converge pas vers 0. C'est absurde.

(iii) ⇒ (iv) $\rho(A) < 1$ donc il existe $\varepsilon > 0$ tel que $\rho(A) + \varepsilon < 1$. Montrons qu'il existe une norme matricielle induite telle que

$$\|A\| \leq \rho(A) + \varepsilon$$

A est trigonalisable, donc il existe $P \in GL_n\mathbb{C}$ telle que $T := P^{-1}AP$ soit triangulaire supérieure. Pour tout réel $\delta > 0$ posons alors

$$D_\delta = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \delta & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \delta^{n-1} \end{pmatrix}$$

Alors

$$T_\delta = D_\delta^{-1} T D_\delta = \begin{pmatrix} t_{11} & \delta t_{12} & \dots & \delta^{n-1} t_{1n} \\ 0 & t_{12} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \delta t_{n-1,n-1} \\ 0 & \dots & 0 & t_{nn} \end{pmatrix}$$

Les coefficients hors diagonaux tendent tous vers 0 avec δ. On peut donc choisir δ tel que $\max\limits_{1 \leq i \leq n-1} \sum\limits_{j=i+1}^{n} |t_{ij}^{(\delta)}| < \varepsilon$

On pose alors $\|x\| := \|D_\delta^{-1} P^{-1} x\|_\infty$. C'est une norme sur $\mathbb{C}^n$, mais aussi sur $\mathbb{R}^n$. Considérons la norme subordonée associée. Alors

$$\begin{aligned} \|A\| &= \sup_{x \neq 0} \frac{\|Ax\|}{\|x\|} \\ &= \sup_{x \neq 0} \frac{\|D_\delta^{-1} P^{-1} A x\|_\infty}{\|D_\delta^{-1} P^{-1} x\|_\infty} \\ &= \sup_{y \neq 0} \frac{\|D_\delta^{-1} P^{-1} A P D_\delta y\|_\infty}{\|y\|_\infty} \\ &\leq \max_{1 \leq i \leq n} \sum_{j=1}^{n} |t_{ij}^{(\delta)}| \leq |t_{kk}| + \varepsilon \end{aligned}$$

Pour un certain indice k.

Or, $|t_{kk}| \leq \rho(T) = \rho(A)$ car T est triangulaire supérieure, semblable à A.

Par suite $\|A\| < 1$ pour cette norme matricielle subordonnée.

(iv) ⇒ (i) Par équivalence des normes en dimension finie il suffit de vérifier que $\|A^k\| \to 0$ pour une norme particulière. On prend donc la norme subordonnée en question :

$$\|A^k\| \leq \|A\|^k \to 0$$

puisque $\|A\| < 1$

□

Proof of 19.2. Posons $B := M^{-1}N$. On introduit le vecteur d'erreur $e_k = x_k - u$ avec u solution de $Ax = b$. Celui-ci vérifie $e_{k+1} = x_{k+1} - u = M^{-1}(Nx_k + b) - u = M^{-1}(Nx_k + b) - M^{-1}(Nu + b) = Be_k$

(⇒) Supposons que $\rho(B) < 1$. Alors d'après le théorème 19.1, $e_k \to 0$ et donc la méthode converge.

(⇐) Réciproquement, si la méthode associée à la décomposition $A = M - N$ converge, alors le vecteur d'erreur e_k tend vers 0, et donc en utilisant de nouveau le théorème 19.1, on a $\rho(B) < 1$. □

19.7 Choix de M et N : Méthode de Gauss-Seidel

Si celle-ci est inversible, on choisit pour matrice M le triangle inférieur de A :

$$\begin{cases} m_{ij} = 0, & \textit{Pour } 1 \leq i < j \leq n, \\ m_{ij} = a_{ij}, & \textit{Pour } 1 \leq j \leq i \leq n. \end{cases}$$

En notant $A = M - N$, le vecteur $x^{(k+1)}$ est solution du système triangulaire inférieur $Mx^{(k+1)} = Nx^{(k)} + b$. D'où l'algorithme de Gauss-Seidel :

$$a_{ii}x_i^{(k+1)} = -\sum_{j=1}^{i-1} a_{ij}x_j^{(k+1)} - \sum_{j=i+1}^{n} a_{ij}x_j^{(k)} + b_i \quad (i = 1, \ldots, n)$$

Remark 19.3. Pour une itération on garde seulement n termes en mémoire.

Theorem 19.4. Si A est symétrique définie positive alors la méthode de Gauss-Seidel converge.

Démonstration. Soit $A \in S_n^{++}(\mathbb{R})$. Une matrice SDP a tous ses termes diagonaux strictement positifs donc M est bien inversible. Soit $\lambda \in \mathbb{C}$ une valeur propre de $G = M^{-1}N$ et $x \in \mathbb{C}^n$ un vecteur propre non nul associé. On décompose $A = D + E - N$ où D est la diagonale de A, E le triangle inférieur strict de sorte que $Nx = \lambda(Dx + Ex)$. . Alors, en notant $\langle . \mid . \rangle$ le produit scalaire hermitien canonique de $\mathbb{C}^n$, on a

$$\begin{aligned} \langle x \mid Ax \rangle &= \langle x \mid Dx \rangle + \langle x \mid Ex \rangle - \langle x \mid Nx \rangle \\ &= (1 - \overline{\lambda})(\langle x \mid Dx \rangle + \langle x \mid Ex \rangle) \end{aligned} \tag{4.18}$$

Puisque $\langle x \mid Ax \rangle > 0$ il vient que $\lambda \neq 1$ et

$$\frac{1}{1-\overline{\lambda}}\langle x \mid Ax\rangle = \langle x \mid Dx\rangle + \langle x \mid Ex\rangle \tag{4.19}$$

En passant à la conjugaison dans 4.18 et en utilisant le fait que A et D sont symétrique réelles et $\overline{E}^T = -N$ il vient :

$$\frac{1}{1-\lambda}\langle x \mid Ax\rangle = \langle x \mid Dx\rangle - \langle x \mid Nx\rangle \tag{4.20}$$

Enfin, (4.19) + (4.20) - (4.18) donne

$$\frac{1-|\lambda|^2}{|1-\lambda|^2}\langle x \mid Ax\rangle = \langle x \mid Dx\rangle$$

Puisque $\langle x \mid Ax\rangle > 0$ et $\langle x \mid Dx\rangle > 0$, on en déduit que $|\lambda| < 1$ et par suite $\rho(G) < 1$.

Conclusion : Si A est SDP réelle, alors la méthode de Gauss-Seidel converge. □

20 Optimisation dans un Hilbert

Références : Ciarlet [CL06]

Definition 20.1. J est coercive ssi $\lim_{\|v\|\to\infty} J(v) = \infty$

20.1 Développement

Theorem 20.2. Soit V un Hilbert séparable, $U \subset V$ une partie non vide, convexe, fermée, et $J : U \to \mathbb{R}$ une fonctionnelle convexe, dérivable. Si U est non borné, on suppose de plus que J est coercive.

Alors, il existe au moins un élément $u \in U$ tel que

$$J(u) = \inf_{v\in U} J(v)$$

20.2 Preuve

Démonstration.

1e étape : On se ramène au cas où U est borné.

Soit $u_0 \in U$. Par coercivité de J il existe r tel que $\|v\| > r \Rightarrow J(v) \geq J(u_0)$.
Alors, $\inf_{v\in V} J(v) \leq J(u_0) \leq J(v)$ pour $\|v\| > r$. Donc,

$$\inf_{v\in U} J(v) = \inf_{v\in U\cap B(0,r)} J(v)$$

[Faire le dessin dans le cas réel au tableau pour fixer les idées]

Posons $U' := U \cap B(0, r)$. Alors U' est borné, convexe (comme intersection de deux convexes), fermée (comme intersection de deux fermés) et le problème initial revient à chercher l'infimum de J sur U'.

Dans la suite on supposera que U est déjà borné.

2eme étape : Une suite minimisante converge faiblement

Soit $(u_k) \in U^{\mathbb{N}}$ une suite minimisante :

$$J(u_k) \to \inf_{v\in U} J(v)$$

.

(u_k) est bornée car U l'est. On note M un majorant. Montrons que l'on peut en extraire une sous-suite qui converge faiblement : Thérème de compacité faible dans les Hilbert.

L'idée est de procéder à une extraction diagonale.

Remarquons tout d'abord que pour tout $v \in V$, l'inégalité de Cauchy-Schwarz donne

$$\begin{aligned}|\langle v, u_k\rangle| &\leq \|v\|\|u_k\| \\ &\leq M_\infty \|v\|\end{aligned}$$

et donc pour tout $v \in V$, la suite $(\langle v, u_n\rangle)$ est bornée.

Par ailleurs, V est séparable. Soit (v_k) une partie dénombrable dense.

— $\langle v_0, u_k\rangle$ est bornée dans $\mathbb{R}$. On peut en extraire une sous-suite convergente $\langle v_0, u_{\varphi_0(k)}\rangle$.

— De même $\langle v_1, u_{\varphi_0(k)}\rangle$ est bornée dans $\mathbb{R}$. On peut en extraire une sous-suite convergente $\langle v_1, u_{\varphi_0\circ\varphi_1(k)}\rangle$.

Posons

$$\varphi : \left\{ \begin{array}{ccc} \mathbb{N} & \mapsto & \mathbb{N} \\ n & \mapsto & \varphi_0 \circ \cdots \circ \varphi_n(n) \end{array} \right.$$

Alors pour tout n, en utilisant la stricte croissance de φ_{n+1},

$$\begin{aligned}\varphi(n+1) - \varphi(n) &= (\varphi_0 \circ \cdots \circ \varphi_n)(\varphi_{n+1}(n+1)) - \varphi_0 \circ \cdots \circ \varphi_n(n) \\ &\geq (\varphi_0 \circ \cdots \circ \varphi_n)(n+1) - \varphi_0 \circ \cdots \circ \varphi_n(n) \\ &> 0\end{aligned}$$

Donc φ est bien une extractrice, et pour tout n ; la suite $(\langle v_n, u_{\varphi(k)}\rangle)_{k\in\mathbb{N}}$ est convergente. Montrons que cela suffit pour avoir la convergence faible.

Soit $v \in V$. Par complétude, il suffit de prouver que $(\langle v, u_{\varphi(n)}\rangle)$ est de Cauchy.

Soit $\varepsilon > 0$. Par densité de $\{v_k\}$, il existe v_k telle que $\|v - v_k\| < \dfrac{\varepsilon}{4M}$

Alors pour $l, m \in \mathbb{N}$,

$$\begin{aligned}|\langle v, u_{\varphi(\ell)}\rangle - \langle v, u_{\varphi(m}\rangle| &= |\langle v, u_{\varphi(\ell)} - u_{\varphi(m}\rangle| \\ &\leq |\langle v_k, u_{\varphi(\ell)} - u_{\varphi(m)}\rangle| + |\langle v - v_k, u_{\varphi(m}\rangle| \\ &\leq |\langle v_k, u_{\varphi(\ell)}\rangle - \langle v_k u_{\varphi(m)}\rangle| + \|v - v_k\|\|u_{\varphi(\ell)} - u_{\varphi(m)}\|\end{aligned}$$

Or, $(\langle v_k, u_{\varphi(n)}\rangle)_{n\in\mathbb{N}}$ converge, donc est de Cauchy. Ainsi, il existe N tel que pour $\ell, m > N$, $|\langle v_k, u_{\varphi(\ell)}\rangle - \langle v_k u_{\varphi(m)}\rangle| \leq \dfrac{\varepsilon}{2}$.

D'où pour $\ell, m > N$,

$$|\langle v, u_{\varphi(\ell)}\rangle - \langle v, u_{\varphi(m}\rangle| < \varepsilon$$

et par suite pour tout v $(\langle v, u_{\varphi(k)}\rangle)_{k\in\mathbb{N}}$ est de Cauchy, donc converge. On note $f(v)$ cette limite.

f définit alors une application linéaire, continue car $|\langle v, u_{\varphi(k)}\rangle| \leq M\|v\|$ pour tout k et donc en passant à la limite il vient $|f(v)| \leq M\|v\|$.

Par le théorème de représentation de Riesz il existe donc u tel que pour tout v, $f(v) = \langle u, v\rangle$ ie $(u_{\varphi(n)})$ converge faiblement vers u.

3eme étape : U est faiblement fermé Soit ρ la projection orthogonale sur U, qui existe car U est convexe fermé dans un $Hilbert$.

Pour tout ℓ, $u_{\varphi(\ell)} \in U$ et donc $\langle \rho u - u, u_{\varphi(\ell)} - \rho u \rangle \geq 0$.

Or, par convergence faible,

$$\langle \rho u - u, u_{\varphi(\ell)} - \rho u \rangle \to \langle \rho u - u, u - \rho u \rangle = -\|\rho u - u\|^2 \leq 0$$

Donc $\|\rho u - u\| = 0$ ie $u \in U$.

4eme étape : Minimisation

x_n minimisante, x_n cv faiblement vers x. On montre que x est dans U convexe fermé blabla. Pour montrer que x_n cv vers le minimum, on pose $C_\beta = \{y \in U \mid J(y) \leq J(u) + \beta\}$ alors $\mathbb{C}_\beta$ est convexe fermé, donc $x \in C_\beta$ pour tout β. On n'a plus besoin de dériver dans des Hilbert.

Prouvons que u est un minimum de J. Il suffit de prouver que

$$J(u) \leq \inf J$$

J est dérivable et convexe donc :

$$J(u) + \langle \nabla J(u), u_{\varphi(\ell)} - u \rangle \leq J(u_{\varphi(\ell)}) \tag{4.21}$$

Or, par convergence faible :

$$\langle \nabla J(u), u_{\varphi(\ell)} \rangle \to \langle \nabla J(u), u \rangle$$

Donc en passant à la limite dans (4.21) il vient :

$$J(u) \leq \liminf J(u_{\varphi(\ell)}) = \inf J$$

D'où le résultat. □

21 [TODO] Ordres moyens

Faire ce dev ou le virer

Références :

— FGN *Analyse 1*

— Tenenbaum *Introduction à la théorie analytique des nombres*

21.1 Contexte :

Definition 21.1. On appelle ordre moyen d'une fonction arithmétique f toute fonction élémentaire de variable rééelle g telle que pour tout x

$$\sum_{n\geq x} f(n) \sim \sum_{n\geq x} g(n)$$

21.2 Développement

22 Formule Sommatoire de Poisson et théorème de Shannon

22.1 Remarques préliminaires

Attention aux conventions pour les leçons sur série/transformée de Fourier. J'ai choisi d'être consistant avec le développement 11 et ce n'est donc pas exactement le même développement que dans les deux références ci-dessous, il faut un peu adapter, mais sinon les calculs sont très similaires.

Pour la leçon sur les séries numériques, on peut faire plutôt l'application au calcul de $\zeta(2)$ plutôt que le théorème de Shannon.

22.2 Références :

— *40 développements d'Analyse*, J et L Bernis [Ber18]

— Zuilly-Queffélec [ZQ13]

22.3 Développement

Theorem 22.1. Soit f un élément de $\mathcal{S}(\mathbb{R})$. Alors

1. Pour tout réel t, on a la formule sommatoire de Poisson :
$$\sum_{n=-\infty}^{+\infty} f(t+2n\pi) = \frac{1}{2\pi}\sum_{k=-\infty}^{+\infty} \widehat{f}(k)e^{ikt}$$
2. Supposons de plus que le support de $\widehat{f}$ soit inclus dans un segment $[-F,F]$ où $F \in \mathbb{R}_*^+$. Si $F < \pi$ alors pour tout réel t :
$$f(t) = \sum_{n=-\infty}^{+\infty} f(n)\frac{\sin((n-t)\pi)}{(n-t)\pi}$$

22.4 Formule sommatoire de Poisson

La somme de la série de fonction définie par f est développable en série de Fourier

Comme f est dans la classe de Schwartz donc on dispose de $M_0 > 0$ tel que pour tout $t \in \mathbb{R}$:
$$|f(t)| \leq \frac{M_0}{1+t^2}$$

En particulier,

$$|f(t+2n\pi)| = O\left(\frac{1}{n^2}\right)$$

Par comparaison avec une série de Riemann on en déduit que pour tout réel t, la série $\sum_{n\in\mathbb{Z}} f(t+2n\pi)$ est convergente. On note $g(t)$ sa somme.

g est $2\pi-$périodique. Pour pouvoir développer g en série de Fourier il suffit de vérifier que g est de classe $\mathcal{C}^1$. Pour cela, on va utiliser un théorème de dérivation terme à terme.

— Pour tout $n \in \mathbb{Z}$, $f(2n\pi + \cdot)$ est de classe $\mathcal{C}^1$.

— Soit K un compact de $\mathbb{R}$ et $N \in \mathbb{N}^*$ tel que $K \subset [-2N\pi, 2N\pi]$. Alors, pour tout $t \in K$ et tout $n \in \mathbb{Z}$ tel que $|n| \geq N+1$ on a

$$1 + |2n\pi + t|^2 \geq (2|n|\pi - |t|)^2 \geq 4\pi^2(|n| - N)^2$$

et donc

$$|f(2n\pi + t)| \leq \frac{M_0}{4\pi^2(|n| - N)^2}$$

Or, la série $\sum_{|n|\geq N+1} \frac{1}{(|n| - N)^2}$ converge, et donc $\sum_{n\in\mathbb{Z}} f(2n\pi+\cdot)$ converge normalement sur K.

— La classe de Schwartz est stable par dérivation, donc on a le même type de majoration pour f' : On dispose de $M_1 > 0$ tel que pour tout $t \in \mathbb{R}$:

$$|f'(t)| \leq \frac{M_1}{1+t^2}$$

et par suite, $\sum_{n\in\mathbb{Z}} f'(2n\pi + \cdot)$ converge normalement sur K.

Par localisation et dérivation terme à terme, on en déduit que g est de classe $\mathcal{C}^1$. Par le *Théorème de Dirichlet*, en notant $c_k(g)$ ses coefficients de Fourier on a donc

$$g(t) = \sum_{k\in\mathbb{Z}} c_k(t) e^{ikt}$$

Calcul des coefficients de Fourier

Soit $k \in \mathbb{Z}$.

$$c_k(g) = \frac{1}{2\pi} \int_0^{\pi} \left(\sum_{k\in\mathbb{Z}} f(2n\pi + t) \right) \exp(-ikt) dt$$

Comme la série converge normalement, donc uniformément, sur $[0, 2\pi]$ l'interversion Somme-Intégrale est licite :

$$c_k(g) = \frac{1}{2\pi} \sum_{k\in\mathbb{Z}} \int_0^{2\pi} f(2n\pi + t) \exp(-ikt) dt$$

Alors par changement de variable,

$$\begin{aligned}\sum_{k=-\infty}^{+\infty}\int_0^{2\pi} f(2n\pi+t)\exp(-ikt)dt &= \sum_{k=-\infty}^{+\infty}\underbrace{e^{2i\pi kn}}_{=1}\int_{2n\pi}^{2(n+1)\pi} f(x)e^{-ikx}dx\\ &= \int_{-\infty}^{\infty} f(x)e^{-ikx}dx\\ &= \widehat{f}(k)\end{aligned}$$

Puisque $f \in \mathcal{S}(\mathbb{R})$.
Finalement,

$$g(t) = \sum_{n=-\infty}^{+\infty} f(t+2n\pi) = \sum_{k\in\mathbb{Z}} c_k(t)e^{ikt} = \frac{1}{2\pi}\sum_{k\in\mathbb{Z}}\widehat{f}(k)e^{ikt}$$

22.5 Théorème d'échantillonnage de Shannon

Supposons le support de $\widehat{f}$ inclus strictement dans $[-\pi,\pi]$. Comme la transformée de Fourier est une bijection de la classe de Schwartz sur elle-même, $\widehat{f} \in \mathcal{S}(\mathbb{R})$ donc par le théorème précédent :

$$\forall \xi \in \mathbb{R},\ \sum_{k=-\infty}^{+\infty}\widehat{f}(\xi+2k\pi) = \sum_{n=-\infty}^{+\infty}\frac{1}{2\pi}\widehat{\widehat{f}}(n)e^{in\xi}$$

Or, d'après la formule d'inversion de Fourier :

$$f(x) = \frac{1}{2\pi}\int_{\mathbb{R}}\widehat{f}(t)e^{itx}dt = \frac{1}{2\pi}\widehat{\widehat{f}}(-x)$$

et donc

$$\frac{1}{2\pi}\widehat{\widehat{f}}(n) = f(-n)$$

puis

$$\sum_{k=-\infty}^{+\infty}\widehat{f}(\xi+2k\pi) = \sum_{n=-\infty}^{+\infty} f(-n)e^{in\xi} = \sum_{m=-\infty}^{+\infty} f(m)e^{-im\xi}$$

Or, si $|\xi| \leq \pi$ et $|k| \geq 1$, $\xi + 2k\pi \notin [-\pi,\pi]$ et par suite $\widehat{f}(\xi+2k\pi) = 0$.
On en déduit

$$\begin{aligned}\widehat{f}(\xi) &= \mathbb{1}_{[-\pi,\pi]}\widehat{f}(\xi)\\ &= \mathbb{1}_{[-\pi,\pi]}\widehat{f}(\xi) + \mathbb{1}_{[-\pi,\pi]}\sum_{k\neq 0}\widehat{f}(\xi+2k\pi)\\ &= \mathbb{1}_{[-\pi,\pi]}\sum_{k\in\mathbb{Z}}\widehat{f}(\xi+2k\pi)\\ &= \mathbb{1}_{[-\pi,\pi]}\sum_{m\in\mathbb{Z}} f(m)e^{-im\xi}\end{aligned}$$

Soit t un réel. En utilisant de nouveau la *Formule d'inversion de Fourier*, on a donc

$$\begin{aligned} f(t) &= \frac{1}{2\pi}\int_{\mathbb{R}} \widehat{f}(\xi)e^{it\xi}d\xi \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \widehat{f}(\xi)e^{it\xi}d\xi \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \left(\sum_{m=-\infty}^{+\infty} f(m)e^{-im\xi}\right) e^{it\xi}d\xi \\ &= \frac{1}{2\pi}\int_{-\pi}^{\pi} \sum_{m=-\infty}^{+\infty} f(m)e^{i(t-m)\xi}d\xi \qquad (4.22) \\ & \qquad (4.23) \end{aligned}$$

Or si $m \in \mathbb{Z}$,

$$|f(m)e^{i(t-m)\xi}| = |f(m)|$$

et la série $\sum_{m\in\mathbb{Z}} f(m)$ est convergente.

Par suite, la série dans 4.22 converge normalement, donc uniformément, sur $[-\pi, \pi]$ et par interversion Série-Intégrale,

$$f(t) = \sum_{m=-\infty}^{+\infty} f(m)\frac{1}{2\pi}\int_{-\pi}^{\pi} e^{i(t-m)\xi}d\xi$$

ie

$$f(t) = \sum_{m=-\infty}^{+\infty} f(m)\frac{sin((m-t)\pi)}{(m-t)\pi}$$

22.6 Application

La formule de poisson peut être utilisée pour calculer des sommes :

Calcul de $\zeta(2)$: Soit $a > 0$ et posons $f_a(x) := e^{-a|x|}$.

f_a est dans la classe de schwartz. Calculons sa transformée de Fourier en découpant l'intégrale en 2 (Les deux morceaux étant intégrables) :

$$\begin{aligned} \widehat{f_a}(\xi) &= \int_{\mathbb{R}} e^{-a|t|}e^{-i\xi t}dt \\ &= \int_0^{\infty} e^{-t(a+i\xi)}dt + \int_{-\infty}^{0} e^{t(a-i\xi)}dt \\ &= \frac{1}{a+i\xi} + \frac{1}{a-i\xi} \\ &= \frac{2a}{a^2+\xi^2} \end{aligned}$$

Soit $\varphi_a(x) := \dfrac{1}{a^2+x^2}$. Alors $\varphi_a(x) = \dfrac{1}{2a}\widehat{f}_a(x)$. Puisque $\varphi_a \in \mathcal{S}(\mathbb{R})$ on peut utiliser le *Théorème d'inversion de Fourier* :

$$\widehat{\varphi_a(x)} = \frac{1}{2a}\widehat{\widehat{f}}_a(x) = \frac{1}{2a}2\pi f_a(-x) = \frac{\pi}{a}e^{-a|x|}$$

Alors, par la *Formule sommatoire de Poisson* on a d'une part :

$$\sum_{n\in\mathbb{Z}} \frac{1}{a^2+4\pi^2n^2} = \frac{1}{2\pi}\sum_{k\in\mathbb{Z}} \frac{\pi}{a}e^{-a|x|} = \frac{1}{2a}\frac{e^a+1}{e^a-1}$$

Et d'autre part :

$$\sum_{n\in\mathbb{Z}} \frac{1}{a^2+4\pi^2n^2} = 2\sum_{n=1}^{\infty} \frac{1}{a^2+4\pi^2n^2} + \frac{1}{a^2}$$

Donc,

$$\sum_{n=1}^{\infty} \frac{1}{a^2+4\pi^2n^2} = \frac{1}{4a}\frac{e^a+1}{e^a-1} - \frac{1}{2a^2} \tag{4.24}$$

Or,

$$\frac{1}{a^2+4\pi^2n^2} \leq \frac{1}{4\pi^2n^2}$$

indépendant de a donc par le *Théorème de convergence dominée*,

$$\lim_{a\to 0}\sum_{n=1}^{\infty} \frac{1}{a^2+4\pi^2n^2} = \sum_{n=1}^{\infty} \frac{1}{4\pi^2n^2} = \frac{1}{4\pi^2}\zeta(2)$$

Calculons la limite du second membre de 4.24 :

$$\begin{aligned}
\frac{1}{e^a-1} &= \left(a + \frac{a^2}{2} + \frac{a^3}{6} + \frac{a^4}{24} + o\left(a^4\right)\right)^{-1} \\
&= \frac{1}{a}\left(1 + \frac{a}{2} + \frac{a^2}{6} + \frac{a^3}{24} + o\left(a^3\right)\right)^{-1} \\
&= \frac{1}{a}\left(1 - \left(\frac{a}{2} + \frac{a^2}{6} + \frac{a^3}{24} + o\left(a^3\right)\right) + \left(\frac{a}{2} + \frac{a^2}{6} + o\left(a^2\right)\right)^2 + o\left(a^3\right)\right) \\
&= \frac{1}{a}\left(1 - \frac{a}{2} - \frac{a^2}{6} - \frac{a^3}{24} + \frac{a^2}{4} + \frac{a^3}{6} + o\left(a^3\right)\right) \\
&= \frac{1}{a} - \frac{1}{2} + \frac{a}{12} + \frac{a^2}{8} + o\left(a^2\right)
\end{aligned}$$

D'où

$$\begin{aligned}\frac{e^a+1}{e^a-1} &= \left(2+a+\frac{a^2}{2}+o\left(a^2\right)\right)\left(\frac{1}{a}-\frac{1}{2}+\frac{a}{12}+\frac{a^2}{8}+o\left(a^2\right)\right)\\ &= \frac{2}{a}-1+\frac{a}{6}+\frac{a^2}{4}+1-\frac{a}{2}+\frac{a^2}{12}+\frac{a}{2}-\frac{a^2}{4}+o(a^2)\\ &= \frac{2}{a}+\frac{a}{6}+o(a)\end{aligned}$$

On en déduit

$$\begin{aligned}\frac{1}{4a}\frac{e^a+1}{e^a-1}-\frac{1}{2a^2} &= \frac{1}{2a^2}+\frac{1}{24}+o(1)-\frac{1}{2a^2}\\ &= \frac{1}{24}+o(1)\to\frac{1}{24}\end{aligned}$$

et finalement

$$\zeta(2)=\frac{4\pi^2}{24}=\frac{\pi^2}{6}$$

23 Marche aléatoire symétrique sur $\mathbb{Z}^d$ [Timé]

23.1 Remarques sur le timing

— Dev long, ne pas traîner, très valorisant et on fait vraiment des proba !

— Dire d'emblée qu'on va regarder des séries de Fourier MultiD, et qu'on admet le calcul d'une intégrale.

— Bien s'attarder sur le début, le lien entre la récurrence de la marche aléatoire et la divergence de l'espérance de N. On fait des proba, on utilise Borel-Cantelli.

— Ça doit nous prendre une colonne 1/2, voire même 2 colonnes.

— Bien regarder le temps à la fin, quitte à rusher.

Timing : 15'08

23.2 Recasages :

— 230 - Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples. (Dans une partie lien avec proba, théorème de Borel Cantelli)

— 246 - Séries de Fourier. Exemples et applications.

— 260 - Espérance, variance et moments d'une variable aléatoire.

— 264 - Variables aléatoires discrètes. Exemples et applications.

23.3 Références

— *Fourier Series and Integrals*, Dym-Mckean [DM85]

23.4 Contexte

Soit $B := (e_1, \dots, e_d)$ la base canonique de $\mathbb{Z}^d$. Soit $E := \{\pm e_i\}$ la symétrisation de B. Soit (X_n) une suite de variables aléatoires iid à valeurs dans E et de loi uniforme. Posons $S_0 := 0$ et $S_n := \sum_{i=1}^{n} X_i$. La suite (S_n) est appelée marche aléatoire symétrique sur $\mathbb{Z}^d$.

23.5 Développement

Theorem 23.1.
Si $d \leq 2$, $\mathbb{P}(S_n = 0 \ i.o) = 1$
Si $d \geq 2$, $\mathbb{P}(|S_n| \to \infty) = 1$

23.6 Preuve

Démonstration. Soit $N := \sum_{n\in\mathbb{N}} \mathbb{1}_{(S_n=0)}$ le nombre de retour en 0 de la marche aléatoire. Faisons la première remarque que $\mathbb{P}(S_n = 0)$ est nulle si n est impair, donc on s'intéressera surtout aux indices pairs.

Soit $A := (S_n = 0\ i.o)$.

$\mathbb{P}(A) = 0$ *ssi* p.s. la marche aléatoire ne revient plus en 0 à partir d'un certain rang.

Le problème est invariant par translation, le résultat reste vrai pour tout point. En particulier, pour tout R, p.s. la marche aléatoire quitte la boule de rayon R, i.e $\mathbb{P}(|S_n| \to \infty) = 1$. Or, par le théorème de Borel-Cantelli, pour avoir $P(A) = 0$ il suffit d'avoir la convergence de $\sum \mathbb{P}(S_n = 0)$, i.e $\mathbb{E}(N) < \infty$.

En fait, c'est équivalent :

Supposons $\sum \mathbb{P}(S_n = 0) = +\infty$. Soit $B := A^c$. Alors, en partitionnant par rapport au dernier passage en 0,

$$\begin{aligned} B &= \bigsqcup_{n\in\mathbb{N}} (S_n = 0, \forall p \geq n+1,\ S_p \neq 0) \\ &= \bigsqcup_{n\in\mathbb{N}} (S_n = 0, \forall p \geq n+1,\ S_p - S_n \neq 0) \end{aligned}$$

Or, $(S_n = 0)$ est indépendant de $(\forall p \geq n+1 S_p - S_n \neq 0)$ puisque ce sont des sommes de variables indépendantes distinctes. Donc

$$\mathbb{P}(B) = \sum_{n\in\mathbb{N}} \mathbb{P}(S_n = 0)\mathbb{P}(\forall p \geq n+1,\ S_p - S_n \neq 0).$$

Or, puisque les X_i ont la même loi,

$$\mathbb{P}(\forall p \geq n+1,\ S_p - S_n \neq 0) = \mathbb{P}\left(\bigcap_{i\geq 1} (X_i \neq 0)\right)$$

est indépendant de n. Notons α cette quantité. Alors,

$$\mathbb{P}(B) = \alpha \sum_{n\in\mathbb{N}} \mathbb{P}(S_n = 0).$$

Puisque $\mathbb{P}(B)$ est borné et $\sum_{n\in\mathbb{N}} \mathbb{P}(S_n = 0) = \infty$, il est nécessaire que $\alpha = 0$, et par suite $\mathbb{P}(B) = 0$ ie $\mathbb{P}(A) = 1$.

On se ramène donc à estimer $E(N)$ et plus particulièrement à calculer sa finitude.

Pour cela, voyons $\mathbb{P}(S_n = k)$ comme le coefficient de Fourier d'une bonne fonction :

Pour tout n et $x \in \mathbb{R}$, $e^{2i\pi<S_n,x>}$ est intégrable et donc

$$f(x) := \sum_{k\in\mathbb{Z}^d} \mathbb{P}(S_n = k) e^{2i\pi<k,x>}$$

est bien définie comme $\mathbb{E}(e^{2i\pi<S_n,x>})$

Or,

$$f(x) = \mathbb{E}\left(\prod_{k=1}^{n} e^{2i\pi<X_k,x>}\right)$$
$$= \prod_{k=1}^{n} \mathbb{E}(e^{2i\pi<X_k,x>})$$

.

Puisque les X_k ont toutes la même loi que $T \sim \mathcal{U}(E)$,

$$f(x) = \left[\mathbb{E}(e^{2i\pi<T,x>})\right]^n.$$

Posons $\varphi(x) := \mathbb{E}(e^{2i\pi<T,x>})$. Alors
$\mathbb{P}(S_n = k)$ est le coefficient de Fourier de f d'ordre k et donc

$$\mathbb{P}(S_n = k) = \int_{[-1,1]^d} \varphi(x)^n e^{-2i\pi<k,x>} dx,$$

et en particulier

$$\mathbb{P}(S_{2n=0}) = \int_{[-1,1]^d} \varphi(x)^{2n} dx$$

Alors

$$\mathbb{E}(N) = \sum_{n\in\mathbb{N}} \mathbb{P}(S_{2n=0})$$
$$= \sum_{n\in\mathbb{N}} \int_{[-1,1]^d} \varphi(x)^{2n} dx$$

Or,

$$\varphi(x) = \sum_{e\in E} \mathbb{P}(T = e) e^{2i\pi<e,x>}$$
$$= \frac{1}{2d} \sum_{k=1}^{d} \left(e^{2i\pi x_k} + e^{-2i\pi x_k}\right)$$
$$= \frac{1}{d} \sum_{k=1}^{d} \cos(2\pi x_k) \in [-1, 1]$$

comme combinaison convexe de points de $[-1, 1]$. Donc $|\varphi(x)| \leq 1$.

De plus, $K := (|\varphi(x)| = 1)$ est l'ensemble des points aux coordonnées à valeurs dans $\{0, 1\}$ ou dans $\{\pm 1/2\}$ et est donc de mesure nulle. Par suite, $|\varphi(x)| < 1$ pp et par suite $|\varphi(x)|^{2n} < 1$ pp.

Alors, par le théorème de Fubini-Tonelli,

$$\mathbb{E}(N) = \int_{[-1,1]^d} \frac{1}{1 - \varphi(x)^2} dx$$

et il suffit d'étudier l'intégrabilité de cette dernière fonction. Elle est continue partout sauf aux points de K. Par symétrie, on peut se limiter à étudier φ^2 sur un voisinage de 0.

$$\begin{aligned}\varphi^2(x) &= \left(\frac{1}{d}\sum_{k=1}^{d} cos(2\pi x_k)\right)^2 \\ &= \left(\frac{1}{d}\sum_{k=1}^{d}(1-\frac{x_k^2}{2}+o(|x_k|^2))\right)^2 \\ &= \left(1-\frac{||x||^2}{2d}+o(||x||^2)\right)^2 \\ &= 1-\frac{||x||^2}{d}+o(||x||^2)\end{aligned}$$

d'où

$$\begin{aligned}\frac{1}{1-\varphi^2(x)} &= \left(\frac{||x||^2}{d}+o(||x||^2)\right)^{-1} \\ &= \frac{d}{||x||^2}+o(\frac{1}{||x||^2}) \qquad\qquad \sim \frac{d}{||x||^2}\end{aligned}$$

Or cette dernière est positive, et n'est intégrable en 0 que si $d \geq 3$.

Conclusion :

- Si $d \leq 2$, l'intégrale diverge ie $N = \infty$ et la marche aléatoire revient presque sûrement une infinité de fois en 0.
- Si $d \geq 3$, l'intégrale converge ie $N < \infty$ et la marche aléatoire diverge presque sûrement.

□

23.7 Post-requis :

Calcul de l'intégrale dans le cas $d = 3$: On passe en coordonnées polaires.

$$\int_{S^2}\frac{dx}{||x||^2} = \int\int\int_{x^2+y^2+z^2\leq 1}\frac{dxdydz}{x^2+y^2+z^2}$$

On passe en coordonnées polaires :
$x = r\cos(\theta)\sin(\varphi)$, $y = r\sin\theta\sin\varphi$, $z = r\cos\varphi$. Posons alors $\psi(r,\theta,\varphi) := (r\cos(\theta)\sin(\varphi), r\sin\theta\sin\varphi$

$$\begin{aligned}\frac{\partial\psi}{\partial r} &= (\cos(\theta)\sin(\varphi), \sin\theta\sin\varphi, \cos\varphi) \\ \frac{\partial\psi}{\partial\theta} &= (-r\sin(\theta)\sin(\varphi), r\cos\theta\sin\varphi, 0) \\ \frac{\partial\psi}{\partial\varphi} &= (r\cos(\theta)\cos(\varphi), r\sin\theta\cos\varphi, -r\sin\varphi)\end{aligned}$$

D'où :

$$\begin{aligned} Jac(\psi) &= \begin{vmatrix} \cos\theta\sin\varphi & -r\sin\theta\sin\varphi & rcos\theta\cos\varphi \\ \sin\theta\sin\varphi & r\cos\theta\sin\varphi & r\sin\theta\cos\varphi \\ cos\varphi & 0 & -r\sin\varphi \end{vmatrix} \\ &= -r^2\sin\varphi \end{aligned}$$

D'où :

$$\begin{aligned} \int_{S^2} \frac{dx}{||x||^2} &= \int_{\theta=0}^{2\pi}\int_{\varphi=0}^{\pi}\int_{r=0}^{1} \frac{r^2\sin(\varphi)}{r^2} dr d\theta d\varphi \\ &= 4\pi \end{aligned}$$

24 SO_3 et les Quaternions [Pseudo-Timé]

24.1 Remarques sur le timing

— Il faut faire les générateurs de $O_n(\mathbb{R})$ et de $SO_n(\mathbb{R})$. Pour s'éviter les calculs pénibles, on peut ne faire que $SO_3(\mathbb{R})$ dans le développement, mais techniquement la preuve est presque la même pour le cas général, juste plus pénible.

— Faire plein de dessins pour les considérations géométriques et donner l'intuition de ce qu'on fait pour les générateurs de $O_3(\mathbb{R})$.

— Pour le développement : On commence par les générateurs de $O_n(\mathbb{R})$, sauf dans la leçon sur les nombres complexes. Pour celle-ci on débute directement par les quaternions, et on fait les générateurs quand on veut prouver la surjectivité. On fait même mieux : On énonce le résultat, on conclut le développement, puis on prouve rapidement le résultat selon le temps qu'il reste.

Timing :

24.2 Recasages :

— 108 - Exemples de parties génératrices d'un groupe. Applications.

— 182 - Applications des nombres complexes à la géométrie.

— 183 - Utilisation des groupes en géométrie.

24.3 Références :

— *Géométrie I*, Berger [Ber90]

— *Cours d'algèbre*, Perrin [Per95]

— *H2G2*, Caldero-Germoni [CG13]

24.4 Contexte

Alors que les nombres complexes sont souvent utilisés pour ramener des problèmes de géométrie à des calculs algébriques, il n'y a pas d'analogue simple pour la dimension 3. On peut dire même plus, les seules algèbres à divisions [3] commutatives sur $\mathbb{R}$ sont $\mathbb{C}$ ou $\mathbb{R}$ lui-même. En revanche, si on accepte de laisser tomber la commutativité, il existe une structure remarquable de $\mathbb{R}$ algèbre à division de dimension 4 : Les quaternions de Hamilton, qu'on notera $\mathbb{H}$.

Les quaternions de module 1 vont alors jouer le même rôle que les complexes de module 1 dans l'étude des rotations planes, et vont ainsi permettre une étude fine de $SO_3(\mathbb{R})$. On peut aussi utiliser les quaternions pour étudier $SO_4(\mathbb{R})$ les isométries directes de l'espace de dimension 4, $\mathbb{R}^4$. Le lecteur intéressé pourra aller lire à ce propos [Ber90] 8.9. ou [CG13] VII.

3. D'aucuns parleraient d'extensions de corps, ce qui est vrai ici mais pour moi un corps *DOIT* être commutatif sans quoi disparaissent beaucoup de propriétés, sur les polynômes notamment. Ce qu'on perd avec $\mathbb{H}$. C'est pour garder un semblant de cohérence que j'ai choisi le terme d'algèbre à divisions.

En pratique Les quaternions sont réellement utilisés, par exemple pour représenter les rotations dans l'espace dans les jeux vidéos.

24.5 Prérequis

Construction des quaternions, associativité, non commutativité, conjugué d'un quaternion, norme (ou module) $N(q) = q\bar{q} = \bar{q}q$, produit scalaire associé, les imaginaires purs ($\mathbb{R}\mathbf{i} \oplus \mathbb{R}\mathbf{j} \oplus \mathbb{R}\mathbf{k}$) forment un espace orthogonal à $\mathbb{R}$ identifié à $\mathbb{R}\mathbf{1}$. L'inverse d'un quaternion de module 1 est son conjugué.

Theorem 24.1. Le centre de $\mathbb{H}$ est réduit à $\mathbb{R}$.

Pour la leçon 182 sur les complexes, on pourra préférer cette réalisation des quaternions de module 1 que l'on trouve par exemple dans [CG13]

Theorem 24.2 (Réalisation matricielle)**.** On considère dans $GL_2(\mathbb{C})$ les sous groupes $\mathbb{R}_+^* := \mathbb{R}_+^* I_2$ et

$$SU(2) := \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}) : |a|^2 + |b|^2 = 1 \right\}$$

Leur intersection est triviale, ils commutent entre eux. On note $H^* \simeq \mathbb{R}_+^* \times SU(2)$ leur produit direct (comme groupes) et on identifie alors $\mathbb{H} \simeq H^* \cup \{0\}$ de sorte que l'on a :

$$\mathbb{H} \simeq \left\{ \begin{pmatrix} a & -\bar{b} \\ b & \bar{a} \end{pmatrix} \in \mathcal{M}_2(\mathbb{C}) : a, b \in \mathbb{C} \right\}$$

alors

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

.

Dans cette représentation matricielle, la conjugaison s'identifie à l'adjonction de matrices, et la norme au déterminant. Alors le groupe des quaternions de norme 1 s'identifie à $SU(2)$ et est isomorphe (et même homéomorphe) à la sphère S^3 en dimension 4. En particulier, $SU(2)$ est (simplement) connexe

Definition 24.3.

- On appelle *réflexion* toute symétrie orthogonale par rapport à un hyperplan.
- On appelle *retournement* (ou *demi-tour*) toute symétrie orthogonale par rapport à un espace de codimension 2 (ie, parallèment à un plan).

24.6 Développement

Theorem 24.4. Soit $n \geq 2$.

— $O_n(\mathbb{R})$ est engendré par les réflexions orthogonales qui ont pour matrice dans une base orthonormée convenable

$$\begin{pmatrix} I_{n-1} & \\ & -1 \end{pmatrix}$$

et plus précisément, toute isométrie est produit d'au plus n réflexions.

Démonstration. — Soit u une isométrie. Notons $\operatorname{Fix} u := \{x \in E \mid u(x) = x\}$ l'espace de ses points fixes, et soit $p_u := n - \dim F_u$. Par récurrence sur p_u on va prouver que u est produit d'au plus p_u réflexions.

$\mathbf{p_u = 0}$ Alors $\operatorname{Fix} u = E$ et $u = Id_E$ qui est le produit de 0 réflexions.

$\mathbf{p_u > 0}$ Soit $x \in (\operatorname{Fix} u)^\perp, x \neq 0$ et posons $y := u(x) \neq x$. L'idée, c'est de trouver un hyperplan H et une réflexion s_H par rapport à cet hyperplan qui envoie y sur x, et qui fixe les points fixes de u, de sorte que $s_H \circ u$ possède strictement plus de points fixes que u.

Insérer un dessin ici.

Sur un dessin, on voit que l'hyperplan médian entre x et y convient. Prouvons le : Comme $\operatorname{Fix} u$ est stable par u et que u est une isométrie, $(\operatorname{Fix} u)^\perp$ est aussi stable par u. Par suite,

$$y \in (\operatorname{Fix} u)^\perp$$

. Par ailleurs, $\|y\| = \|u(x)\| = \|x\|$ et donc

$$\langle x - y \mid x + y \rangle = 0$$

ie

$$x - y \perp x + y$$

.

Posons $H := (x-y)^\perp$ et soit s_H la réflexion par rapport à H. Alors, $s_H(x-y) = y-x$ et $s_H(x+y) = x+y$ donc $s_H(y) = x$. De plus, comme $x, y \in (\operatorname{Fix} u)^\perp$, il en est de même pour $x-y$. Par suite, $\operatorname{Fix} u \subset H$ et donc s_H stabilise $\operatorname{Fix} u$. On en déduit que $s_H \circ u$ a strictement plus de points fixes que u et donc $p_{s_H \circ u} < p_u$. Par récurrence, il est produit d'au plus $p_u - 1$ réflexions, et donc $u = s_H \circ (s_H \circ u)$ est produit d'au plus p_u réflexions.

Cas particulier de $SO_3(\mathbb{R})$ Soit $u \in SO_3(\mathbb{R})$. u est produit d'au plus 3 réflexions. Puisque $\det(u) = 1$, on en déduit que si u est différent de l'identité, u est produit de deux réflexions : $u = \tau\tau' = (-\tau)(-\tau')$. Or, en dimension 3, l'opposée d'une réflexion d'hyperplan H est un retournement d'axe $H^\perp$. Donc u est produit de deux retournements.

□

Theorem 24.5. Il existe un isomorphisme *explicite* de groupes

$$SU(2)/\{\pm I_2\} \simeq SO_3(\mathbb{R})$$

— *Démonstration.*

Action de $SU(2)$ sur $\mathbb{H}$ est isométrique : $SU(2)$ agit sur $\mathbb{H}$ par conjugaison. On note φ_h l'automorphisme associé à la matrice $h \in SU(2)$:

$$\varphi_h : \left\{ \begin{array}{ccc} \mathbb{H} & \to & \mathbb{H} \\ u & \mapsto & huh^{-1} \end{array} \right.$$

φ_h est linéaire et respecte la norme : $N(huh^{-1}) = \det(huh^{-1}) = \det(u) = N(u)$. C'est donc une *isométrie*.

Restriction aux imaginaires purs On note $\mathbb{I} := \mathbb{R}\mathbf{i} \oplus \mathbb{R}\mathbf{j} \oplus \mathbb{R}\mathbf{k} = (\mathbb{R}\mathbf{1})^\perp$ l'espace des imaginaires purs. Comme $\mathbf{1}$ est central dans $\mathbb{H}$, pour tout $h \in SU(2)$, φ_h stabilise $\mathbb{R}$ et par conséquent φ_h stabilise $\mathbb{R}^\perp = \mathbb{I}$. Par restriction, φ_h définit une isométrie de $\mathbb{I}$ qui s'identifie à $\mathbb{R}^3$. Par suite, on a le morphisme

$$\varphi : \left\{ \begin{array}{ccc} SU(2) & \to & O(\mathbb{I}) \simeq O_3(\mathbb{R}) \\ h & \mapsto & \varphi_h \end{array} \right.$$

On précise l'image φ est continue, donc par composition $\det \circ \varphi : SU(2) \to \{\pm 1\}$ est continue. Or, $SU(2)$ (homéomorphe à S^3) est connexe, donc $\det \circ \varphi(SU(2))$ est connexe et par suite constant. Comme de plus $\varphi_{I_2} = Id$ est de déterminant 1 on en déduit que $det \circ \varphi(SU(2)) = \{1\}$, ie

$$\operatorname{Im} \varphi \subset SO_3(\mathbb{R})$$

Le morphisme est surjectif D'après (24.4) il suffit de prouver que tous les retournements de $SO_3(\mathbb{R})$ sont dans $\operatorname{Im} \varphi$.

Soit $h \in \mathbb{I} \cap S^3$ et r_h le retournement d'axe $\mathbb{R}h$. Montrons que $r_h = \varphi_h$:

φ_h stabilise $\mathbb{R}h$ En effet, $\varphi_h(h) = hhh^{-1} = h$.

Si $\langle h, h' \rangle = 0$ alors $\varphi_h(h') = -h'$ En effet, fixons h' orthogonal à h, ie $h'\bar{h} + h\bar{h'} = 0$. Donc puisqu'ils sont dans $\mathbb{I}$, $h'(-h) + h(-h') = 0$ d'où on déduit immédiatement $hh'h^{-1} = -h'$.

Le noyau $\operatorname{Ker} \varphi = Z(\mathbb{H}) \cap SU(2) = \mathbb{R} \cap SU(2) = \{\pm 1\}$

Conclusion Par le théorème de factorisation, φ induit un isomorphisme

$$SU(2)/\operatorname{Ker} \varphi \simeq \operatorname{Im} \varphi$$

ie

$$SU(2)/\{\pm I_2\} \simeq SO_3(\mathbb{R})$$

□

24.7 Postrequis

— On a ce théorème plus général sur les générateurs de $SO_n(\mathbb{R})$:

> **Theorem 24.6.** Si $n \geq 3$, $SO_n(\mathbb{R})$ est engendré par les retournements orthogonaux (= demi-tours) qui ont pour matrice dans une base orthonormée convenable
> $$\begin{pmatrix} I_{n-2} & \\ & -I_2 \end{pmatrix}$$
> plus précisément toute isométrie directe est produit d'un nombre pair de retournements orthogonaux.

Démonstration. Soit $u \in SO_n(\mathbb{R})$. Il est produit de k réflexions. Puisque $\det u = 1$, on en déduit que $k = 2p$ est pair. Quitte à simplifier, on peut prendre k minimal de sorte que deux réflexions qui se suivent dans le produit sont distinctes. Il suffit donc de prouver le lemme suivant

> **Lemma 24.7.** Soient H et H' deux hyperplans distincts. On note $s_H, s_{H'}$ les symétries hyperplanes (=réflexions) associées. Alors il existe un couple (r, r') de retournements telles que $s_H \circ s_{H'} = r \circ r'$.

Démonstration. Posons $F := H \cap H'$. Puisque les hyperplans sont distincts, $H + H' = \mathbb{R}^n$ et donc $\dim F = \dim H + \dim H' - \dim(H + H') = n - 1 + n - 1 - n = n - 2$. Soit $(e_1, \dots, e_{n-2})$ une base orthonormée de F qu'on complète en une base orthonormée de $\mathbb{R}^n$ $(e_1, \dots, e_n)$. On définit alors r et r' par

$$\begin{array}{ccc} r(e_i) = e_i & r'(e_i) = e_i & 1 \leq i \leq n-3 \\ r(e_{n-2}) = -e_{n-2} & r(e_{n-1}) = s_H(e_{n-1}) & r(e_n) = s_H(e_n) \\ r'(e_{n-2}) = -e_{n-2} & r'(e_{n-1}) = s_{H'}(e_{n-1}) & r'(e_n) = s_{H'}(e_n) \end{array}$$

Préciser cette preuve

Notons que e_{n-1}, e_n appartiennent à H ou H', mais pas le même en même temps, et pas les deux. Par exemple, $e_{n-1} \in H' \backslash H$ et $e_n \in H \backslash H'$. Par suite, $(e_1, \dots, e_{n-2}, e_{n-1})$ est une base orthonormée de H' et $(e_1, \dots, e_{n-2}, e_n)$ est une base orthonormée de H. On a de plus, $e_{n-1} \in H' \cap H^\perp$ et de même $e_n \in H \cap H'^\perp$. Alors, $s_H \circ s_{H'} = r \circ r'$ sur F et sur $F^\perp$ donc sur $\mathbb{R}^n$. Il reste à prouver que r et r' sont bien des retournements. Or, les matrices de r et r' dans la base orthonormée $(e_1, \dots, e_n)$ de $\mathbb{R}^n$ sont respectivement

$$R = \begin{pmatrix} I_{n-3} & & & \\ & -1 & & \\ & & -1 & \\ & & & 1 \end{pmatrix} R' = \begin{pmatrix} I_{n-3} & & & \\ & -1 & & \\ & & 1 & \\ & & & -1 \end{pmatrix}$$

Ce sont donc bien des retournements, par rapport à $\mathrm{Vect}(e_1, \dots, e_{n-3}) \oplus^\perp e_n$ et $\mathrm{Vect}(e_1, \dots, e_{n-3}) \oplus^\perp e_{n-1}$ respectivement. □

□

— On peut faire une interprétation topologique de ce résultat : Puisque le morphisme est en plus continu et de réciproque continu, $SO_3(\mathbb{R})$ est alors homéomorphe à l'espace projectif $\mathbb{P}^3(\mathbb{R})$, quotient $S^3/\{\pm I_2\}$ de la sphère S^3 par antipodie. Comme S^3 est simplement connexe (la preuve se fait en invoquant le théorème de Van Kampen, le lecteur intéressé pourra trouver ce résultat dans moult ouvrage de topologie algébrique), et comme $\{\pm I_2\}$ est discret, on en déduit que $SU(2)$ est le revêtement universel de SO_3 (à deux feuillets) et donc que le groupe fondamental de ce dernier est $\mathbb{Z}/2\mathbb{Z}$. C'est grâce à cela que l'on peut faire des clefs de bras [4]. Un lacet non trivial peut être trouvé de la façon suivante : Prendre une assiette dans la main, posée à plat [5]. Faire tourner la main de 360° autour de la normale passant par le centre de l'assiette. Le bras aura nécessairement tourné, et est un peu tordu, mais l'assiette est restée à plat. C'est donc bien un lacet non trivial. Ce que nous dit ce théorème c'est qu'une seconde rotation de 360° autour du même axe et dans le même sens ramène le bras à sa position initiale au lieu de le tordre deux fois plus !

4. Comment ça les Judoka n'ont que faire des revêtements universels ?
5. L'auteur de ces lignes n'est pas responsable des bris d'assiettes.

25 Loi de la réciprocité quadratique [Timé]

25.1 Remarques sur le timing

— Le dev passe vraiment très bien en 15 min, même en insistant plus sur telle ou telle partie du dev selon la leçon (plutôt actions de groupes, plutôt formes quadratiques, plutôt dénombrement de solution d'équation).

— Partie 1 sur la première colonne, l'action de $\mathbb{Z}/p\mathbb{Z}$ est claire. On fait un schéma pour expliquer les deux types de stabilisateurs, on énonce l'équation aux classes et bim.

— Sur la colonne 2, on blablatte sur la classification des formes quadratiques, pour bien faire comprendre qu'on se sert de plein de résultats, et pourquoi on va chercher une forme équivalente.

— Sur la colonne 3, on fait le dénombrement de X'. C'est des méthodes combinatoires, le jury va aimer, on n'écrit pas trop. On peut faire des accolades sous les expressions si on veut mais pas plus.

— Enfin, sur la colonne 4, on égalise les deux cardinaux, on trouve la réciprocité quadratique modulo p et on remonte à $\mathbb{Z}$.

Timing : 15'08

25.2 Recasages :

— 101 - Groupe opérant sur un ensemble. Exemples et applications.

— 123 - Corps finis. Applications.

— 126 - Exemples d'équations en arithmétique.

— 170 - Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

— 190 - Méthodes combinatoires, problèmes de dénombrement.

25.3 Référence :

H2G2 tome 1 [CG13] (Attention, il y a une erreur dans la preuve) ou [CG17a]

25.4 Développement

Theorem 25.1. Soit p, q deux nombres premiers impairs distincts. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{2}}$$

25.5 Preuve

L'idée est de procéder à un double dénombrement. On va en effet dénombrer de deux façons différentes le cardinal de la sphère unité de $\mathbb{F}_q^p$:

$$X := \{(x_1, \ldots, x_p) \in \mathbb{F}_q^p \mid \sum_{i=1}^{p} x_i^2 = 1\}$$

D'une part on exploite une action de groupe et l'équation aux classes, et d'autre part on va chercher un ensemble en bijection avec X et dont le cardinal est plus facile à déterminer. Pour cela on va exploiter la caractérisation des formes quadratiques sur des corps finis.

— On fait agir $\mathbb{Z}/p\mathbb{Z}$ par permutation circulaire sur X :

$$k.(x_1, \ldots, x_p) = (x_{1+k}, \ldots, x_{n+k})$$

où les indices sont pris modulo p. Le stabilisateur $Stab(x)$ d'un élément est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$ et comme p est premier, $Stab(x) = \{1\}$ ou $Stab(x) = \mathbb{Z}/p\mathbb{Z}$. Les éléments $\tilde{x} \in X$ de stabilisateur $\mathbb{Z}/p\mathbb{Z}$ sont uniquement de la forme $(x, \ldots, x)$ et par conséquent tous les autres éléments ont un stabilisateur trivial. Le nombre d'orbites à stabilisateur non trivial est donc l'ensemble des solutions à l'équation $px^2 = 1$ dans $\mathbb{F}_q$:

$$\left(\frac{p}{q}\right) + 1$$

et le cardinal des autres orbites est divisible par p. D'après l'équation aux classes on a donc

$$|X| = 1 + \left(\frac{p}{q}\right) \mod p. \tag{4.25}$$

— Cherchons une bijection de domaine X. On va chercher exploiter le caractère espace vectoriel de $\mathbb{F}_q^p$ et donc chercher un automorphisme. On va chercher une deuxième forme quadratique, équivalente à la norme euclidienne. D'après la classification des formes quadratiques sur des corps finis, il suffit de trouver une forme quadratique dont la matrice a même rang et même déterminant.

Or, la matrice du carré de la norme est l'identité, de rang p et de déterminant 1. Posons alors la matrice A de taille p :

$$A := \begin{pmatrix} 0 & 1 & & & & & \\ 1 & 0 & & & & & \\ & & 0 & 1 & & & \\ & & 1 & 0 & & & \\ & & & & \ddots & & \\ & & & & & 0 & 1 \\ & & & & & 1 & 0 \\ & & & & & & a \end{pmatrix}$$

avec $a := (-1)^d$ où $d = \dfrac{p-1}{2}$. Elle est bien symétrique, de rang p et de déterminant $1 = (-1)^{(p-1)/2}a$ (donc même discriminant). Elles sont donc congruentes et on dispose de $P \in GL_p(\mathbb{F}_q)$ telle que $A = P^T I_p P = P^T P$. Par suite $u \mapsto P^{-1}u$ est une bijection, et l'image de $X = \{x \mid x^T x = 1\}$ est

$$\begin{aligned} X' &= \{x \in F_q^p \mid x^T A x = 1\} \\ &= \{(y_1, z_1, y_2, z_2, \ldots, y_d, z_d, t) \in F_q^p \mid 2(y_1 z_1 + \cdots + y_d z_d) + at^2 = 1\} \\ &= \{(y_1, z_1, y_2, z_2, \ldots, y_d, z_d, t) \in F_q^p \mid 2\langle \vec{y}, \vec{z} \rangle + at^2 = 1\} \end{aligned}$$

Dénombrement de X' : Écrivons $X' = Y_0 \bigsqcup Z$ avec

$$Y_0 = \{(y_1, z_1, y_2, z_2, \ldots, y_d, z_d, t) \in X' \mid \vec{y} = 0\}$$

et Z son complémentaire.

- Un élément de Y_0 est défini ssi l'équation $at^2 = 1$ a une solution. Il en existe $1 + \left(\frac{a}{q}\right) = 1 + a^{(q-1)/2}$. Pour chaque solution il y a q^d choix pour $\vec{z}$. On en déduit que $|X_0| = q^d(1 + a^{(q-1)/2})$
- Pour construire un élément de Z il faut choisir $\vec{y} \neq 0$ (il y a $q^d - 1$ tels choix) et t (q possibilités), puis $\vec{z}$ dans l'hyperplan affine

  $$2\langle \vec{y}, \cdot \rangle = 1 - at^2$$

  (On utilise ici que q est impair et donc 2 est bien inversible). Il y a donc q^{d-1} possibilités pour $\vec{z}$. Finalement, $|Z| = (q^d - 1)q^d$

On en déduit que

$$\begin{aligned} |X'| &= |X_0| + |Z| \\ &= q^d(1 + a^{(q-1)/2}) + (q^d - 1)q^d \\ &= q^d(q^d + a^{(q-1)/2} \\ &= q^d(q^{(p-1)/2} + (-1)^{(p-1)(q-1)/2}) \end{aligned} \tag{4.26}$$

Par suite, en égalisant 4.25 et 4.26 on en déduit

$$\begin{aligned} |X| = q^d(q^{(p-1)/2} + (-1)^{(p-1)(q-1)/2}) &= 1 + \left(\frac{p}{q}\right) \mod p \\ = q^{(p-1)/2}(q^{(p-1)/2} + (-1)^{(p-1)(q-1)/2}) &= 1 + \left(\frac{p}{q}\right) \mod p \\ = \left(\frac{q}{p}\right)\left[\left(\frac{q}{p}\right) + (-1)^{(p-1)(q-1)/2}\right] &= 1 + \left(\frac{p}{q}\right) \mod p \end{aligned}$$

Et puisque $\left(\frac{p}{q}\right) \in \{\pm 1\}$ il vient

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/2} \mod p$$

Comme p est impair et que les deux membres de l'égalité sont égaux soit à 1 soit à -1 on peut relever l'égalité dans $\mathbb{Z}$. D'où le résultat.

25.6 Questions possibles

— À quoi sert la loi de réciprocité quadratique ?

— Pourquoi on avait supposé p et q impairs ?

— Que sont les lois complémentaires ? Idées de la preuve ?

26 Convergence de séries de variables aléatoires

Référence : Lacroix, Mazliak [LM06]

26.1 Développement :

Theorem 26.1.
Soit (X_n) une suite de variables aléatoires indépendantes, centrées, admettant un moment d'ordre 2. On pose

$$S_n := \sum_{k=1}^{n} X_k$$

Alors, si

$$\sum \mathbb{E}(X_k) < \infty,$$

La suite (S_n) converge presque sûrement.

Remark 26.2. Variante pour la leçon 264 : Série à signe aléatoires

Theorem 26.3.
Soit $(a_n) \in \ell^2(\mathbb{C})$ et soit (ϵ_n) une suite de signes aléatoires indépendants. Alors, la série $\sum \varepsilon_n a_n$ converge presque sûrement.

26.2 Preuve

Démonstration. On commence par prouver que (S_n) converge dans L^2. Par complétude il suffit de prouver que la suite est de Cauchy dans L^2 :

$$\begin{aligned}
\mathbb{E}\left(|S_{n+p} - S_n|^2\right) &= \mathbb{E}\left(\left|\sum_{k=n+1}^{n+p} X_k\right|^2\right) \\
&= \mathbb{E}\left(\sum_{k=n+1}^{n+p}\sum_{j=n+1}^{n+p} X_k \bar{X}_j\right) \\
&= \sum_{k=n+1}^{n+p}\sum_{j=n+1}^{n+p} \mathbb{E}\left(X_k \bar{X}_j\right)
\end{aligned}$$

par linéarité.
Donc :

$$||S_{n+p} - S_n||_2^2 = \sum_{k=n+1}^{n+p} \mathbb{E}(|X_k|^2) + \sum_{j\neq k} \mathbb{E}\left(X_k\right)\mathbb{E}\left(\bar{X_j}\right)$$

Par indépendance. Or, puisque les variables sont centrées, $\mathbb{E}(X_k) = 0$ pour tout k.
Par suite :

$$\begin{aligned} ||S_{n+p} - S_n||_2^2 &= \sum_{k=n+1}^{n+p} \mathbb{E}(|X_k|^2) \\ &\leq \sum_{k=n+1}^{\infty} \mathbb{E}(|X_k|^2) \\ &\varepsilon \end{aligned}$$

pour n suffisamment grand. Donc la suite (S_n) converge dans L^2, et par suite il existe une sous suite qui converge presque-sûrement.

Pour prouver que la suite entière converge p.s. on va utiliser le lemme suivant :

Lemma 26.4.

$$\mathbb{P}(\max_{1\leq k\leq n} |S_k| \geq \varepsilon) \leq \frac{\mathbb{E}(|S_n|^2)}{\varepsilon^2}$$

Proof. lemma Pour $1 \leq k \leq n$ posons

$$A_k := (|S_1| < \varepsilon, |S_2| < \varepsilon, \ldots, |S_{k-1}| < \varepsilon, |S_k| \geq \varepsilon)$$

Alors,

$$(\max_{1\leq k\leq n} |S_k| \geq \varepsilon) = \bigsqcup_{k=1}^{n} A_k$$

Par ailleurs, $S_n - S_p = \sum_{k=p+1}^{n} X_k$ est indépendant de $S_p \mathbb{1}_{A_p}$;
et $\mathbb{E}\left(S_n - S_p\right) = 0$ donc :

$$\begin{aligned} \mathbb{E}\left(|S_n|^2 \mathbb{1}_{A_p}\right) &= \mathbb{E}\left(|S_n - S_p + S_p|^2 \mathbb{1}_{A_p}\right) \\ &= \mathbb{E}\left(|S_n - S_p|^2 \mathbb{1}_{A_p}\right) + \mathbb{E}\left(|S_p|^2 \mathbb{1}_{A_p}\right) + 2\mathfrak{R}\mathbb{E}\left((S_n - S_p)\overline{S_p}\mathbb{1}_{A_p}\right) \\ &= \mathbb{E}\left(|S_n - S_p|^2 \mathbb{1}_{A_p}\right) + \mathbb{E}\left(|S_p|^2 \mathbb{1}_{A_p}\right) + 2\mathfrak{R}\left[\mathbb{E}\left(S_n - S_p\right)\mathbb{E}\left(\overline{S_p}\mathbb{1}_{A_p}\right)\right] \\ &= \mathbb{E}\left(|S_n - S_p|^2 \mathbb{1}_{A_p}\right) + \mathbb{E}\left(|S_p|^2 \mathbb{1}_{A_p}\right) \\ &\geq \mathbb{E}\left(|S_p|^2 \mathbb{1}_{A_p}\right) \\ &\geq \varepsilon^2 \mathbb{P}(A_p) \end{aligned}$$

En sommant sur p et en utilisant $\sum_{p=1}^{n} \mathbb{1}_{A_p} \leq 1$ on a : $|S_n|^2 \sum_{p=1}^{n} \mathbb{1}_{A_p} \leq |S_n|^2$ d'où

$$\mathbb{E}(|S_n|^2) \geq \varepsilon^2 \max_{1\leq k\leq n} [|S_k| \geq \varepsilon]$$

d'où le résultat.

À présent, prouvons la convergence presque sûre. Pour cela, il suffit de prouver que (S_n) est presque sûrement de Cauchy, et on va utiliser le lemme de Borel-Cantelli.

Comme $S_n \to S$ dans L^2, on peut construire par récurrence une suite strictement croissante d'entiers (n_k) vérifiant $\mathbb{E}(|S - S_{n_k}|^2) < \dfrac{1}{2^k}$.

Soit $\varepsilon > 0$. Par le lemme,

$$\mathbb{P}(\max_{1\leq p\leq n} |S_p - S_{n_k}| \geq \varepsilon) \leq \frac{\mathbb{E}(|S_n - S_{n_k}|^2)}{\varepsilon^2}$$

De plus, $S_n \to S$ dans L^2, donc $\mathbb{E}\left(|S_n - S_{n_k}|^2\right) \to \mathbb{E}(|S - S_n|)$ Et par limite croissante dans le membre de gauche,

$$\begin{aligned}\mathbb{P}(\max_{1\leq p} |S_p - S_{n_k}| \geq \varepsilon) &\leq \frac{\mathbb{E}(|S - S_{n_k}|^2)}{\varepsilon^2} \\ &\leq \frac{1}{\varepsilon^2}\frac{1}{2^k}\end{aligned}$$

Posons $B_p := (\max_{1\leq p} |S_p - S_{n_k}| \geq \varepsilon)$.

Alors, la série de terme général $P(B_p)$ converge, donc par le lemme de Borell-Cantelli, $\mathbb{P}(\cap_{n\in\mathbb{N}} \cup_{p\geq n} B_p) = 0$ ie $\mathbb{P}(\cup_{n\in\mathbb{N}} \cap_{p\geq n} \overline{B_p}) = 1$.

Ainsi, presque sûrement il existe N tel que $sup_{p\geq N}|S_p - S_N| < \varepsilon$, donc pour $n \geq N$; $|S_n - S_{n+p}| < 2\varepsilon$ ps.

Conclusion : (S_n) est presque sûrement de Cauchy, et donc (S_n) converge presque sûrement.

□

27 Équation différentielle via H^1

27.1 Références

— Berthelin [Ber17]

27.2 Contexte

Cette équation est en fait le cas général d'une équation linéaire d'ordre 2 puisqu'elles peuvent toutes se ramener à cette forme. Ce résultat est donc très intéressant, parce qu'il signifie que modulo quelques hypothèses de régularité sur les coefficients, l'équation différentielle avec une condition de nullité au bord admet une unique solution.

27.3 Prérequis

Il faut connaître les Sobolev H^1 et H^1_0 en particulier et leurs interactions (densité etc). Par ailleurs, il faut connaître l'inégalité de Poincaré sur H^1_0 et savoir la redémontrer si besoin. Il faut aussi savoir que tout élément de H_1 possède un représentant continu (et avoir une idée de la preuve).

Dans la suite on considèrera donc que toutes les fonctions considérées dans H^1 seront en réalité continues.

27.4 Développement

Soit $I = [0,1]$, $p \in \mathcal{C}^1, q, f \in \mathcal{C}^0$. On considère l'équation différentielle avec condition de nullité au bord :

$$\begin{cases} (-p'u')' + qu = f \\ u(0) = u(1) = 0 \end{cases} \tag{4.27}$$

Theorem 27.1. On suppose que $p > 0$ et $q > 0$. Alors l'équation (4.27) admet une unique solution.

27.5 Preuve

Démonstration. La preuve se fait en plusieurs temps. Tout d'abord on montre que l'équation admet une unique solution faible dans H^1_0, puis on lui trouve une plus grande régularité, avant enfin de prouver qu'elle est solution forte.

Solution faible

On considère H^1 muni du produit scalaire

$$\langle u, v \rangle := \int_0^1 uv + \int_0^1 u'v'$$

et H_0^1 normé par $\|u\|_{H_0^1} := \|u'\|_{L^2}$.

D'après l'inégalité de Poincaré, il existe C tel que

$$\|u\|_{L^2} \leq C\|u'\|_{L^2}$$

Alors,

$$\begin{aligned}\|u\|_{H_0^1}^2 = \|u'\|_{L^2}^2 \leq \|u'\|_{L^2}^2 + \|u\|_{L^2}^2 = \|u\|_{H^1}^2 \\ \leq (1+C)\|u'\|_{L^2}^2 = (1+C)\|u\|_{H_0^1}\end{aligned}$$

Donc sur H_0^1, la norme spécifique est équivalente à la norme issue de H^1.

Comme p est continue sur le compact $[0,1]$, et est strictement positive, il existe $\alpha > 0$ tel que $p(t) \geq \alpha > 0$ pour $t \in I$.

Posons

$$\begin{cases} B(u,v) & := & \displaystyle\int_0^1 pu'v' + \int_0^1 quv \\ \varphi(v) & := & \displaystyle\int_0^1 fv \end{cases}$$

respectivement définies sur $H_0^1 \times H_0^1$ et sur H_0^1.

B est bilinéaire, symétrique et puisque $q \geq 0$

$$\begin{aligned}B(u,u) = \int_0^1 pu'^2 + \int_0^1 qu^2 \geq \alpha \int_0^1 u'^2 \\ = \alpha\|u\|_{H_0^1}^2\end{aligned}$$

Donc B est définie positive : C'est un produit scalaire. De plus,

$$\begin{aligned}B(u,u) \leq \max(\|p\|_\infty, \|q\|_\infty)\|u\|_{H_1}^2 \\ \leq C^2 M\|u\|_{H_0^1}\end{aligned}$$

par l'inégalité de Poincaré.

Donc, B définit encore une norme sur H_0^1, équivalente aux deux autres. En particulier, (H_0^1, B) est un espace de Hibert.

Par ailleurs, φ est linéaire et en utilisant l'inégalité de Cauchy Schwarz et l'inégalité de Poincaré, on a :

$$|\varphi(v)| \leq \|f\|_{L^2}\|v\|_{L^2} \leq C\|f\|_{L^2}\|v\|_{H_0^1}$$

Par suite, φ est une forme linéaire, continue sur H_0^1 (et $\|\varphi\| \leq C\|f\|_{L^2}$)

Par le théorème de représentation de Riesz, il existe donc un unique $u_0 \in H_0^1(I)$ tel que

$$\varphi(v) = B(u_0, v)$$

pour tout $v \in H_0^1$.

C'est à dire, qu'il existe une unique solution faible au problème.

Gagner plus de régularité Pour tout $v \in \mathcal{C}_c^\infty$,

$$\int_0^1 pu_0'v' = \int_0^1 fv - \int_0^1 qu_0v = \int_0^1 (f - qu_0)v$$

Donc $pu_0' \in L^2$ admet une dérivée faible $-(f - qu_0) \in L^2$. En particulier $pu_0' \in H^1$.

Comme $p > 0$ et est $\mathcal{C}^1$, $\dfrac{1}{p}$ est aussi de classe $\mathcal{C}^1$.

Donc $u_0' = \dfrac{1}{p}(pu_0') \in H^1$ comme produit d'une fonction $\mathcal{C}^1$ par une fonction dans H^1.

Donc u_0' est continu, et par suite u_0 est $\mathcal{C}^1$.

Or, $(pu_0')' = -(f - qu_0)$ est continue ie pu_0' est $\mathcal{C}^1$. Par suite, u_0' est aussi $\mathcal{C}^1$ ie

$$u_0 \in \mathcal{C}^2$$

.

Solution forte pu_0' est $\mathcal{C}^1$ de dérivée $-(f - qu_0)$ ie $(-pu_0')' = f - qu_0$.

Alors

$$(-pu_0')' + qu_0 = f$$

Comme de plus $u_0 \in H_0^1$ on en déduit que $u_0(0) = u_0(1) = 0$.

Conclusion Donc u_0 est bien solution forte du problème. Par unicité de la solution faible, on en déduit que l'équation différentielle possède une unique solution. □

28 Théorème de Sophie-Germain

28.1 Recasages :

— 121 - Nombres premiers. Applications.

— 126 - Exemples d'équations en arithmétique.

28.2 Référence

FGN Algèbre 1, [FN07a]

28.3 Développement

Theorem 28.1. Soit p premier tel que $q := 2p+1$ est aussi premier. Alors si $(x, y, z) \in \mathbb{Z}^3$ est tel que $x^p + y^p + z^p = 0$ alors $xyz \equiv 0[p]$.

Démonstration. Soit $(x, y, z) \in \mathbb{Z}^3$ une telle solution et supposons par l'absurde que $xyz \not\equiv 0[p]$.

1ere étape : On se ramène à x,y,z premiers entre eux deux à deux

Soit $\delta := pgcd(x, y, z)$. Alors en posant $x' := \frac{x}{\delta}, y' := \frac{y}{\delta}, z' := \frac{z}{\delta}$ on en déduit que $x'^p + y'^p + z'^p = 0$ et $pgcd(x', y', z') = 1$. Puisque $xyz \not\equiv 0[p]$ on peut supposer que $pgcd(x, y, z) = 1$. Supposons $pgcd(x, y) > 1$ et soit d un diviseur premier de $pgcd(x, y)$. Alors d divise $x^p + y^p = (-z)^p$ donc d divise z^p et puisque d est premier il divise aussi z. Par conséquent, d divise $pgcd(x, y, z) = 1$. Absurde. Le même raisonnement montre que x, y, z sont en fait premiers entre eux deux à deux.

2ème étape : Les somme deux à deux sont des puissances p-ième

$$(-x)^p = y^p + z^p = (y + z)\sum_{k=0}^{p-1}(-z)^{p-1-k}y^k = (y + z)u$$

$y + z$ et u sont premiers entre eux car si p' est un diviseur commun alors

— $p' \mid y + z$ donc $p' \mid x^p$ et par suite $p' \mid x$.

— Comme $y + z \equiv 0[p']$ on a

$$u = \sum_{k=0}^{p-1}(-z)^{p-1-k}y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv py^{p-1}[p']$$

Or, $u \equiv 0[p']$ et par suite $py^{p-1} \equiv 0[p']$ ie $p' \mid py^{p-1}$. Comme p' est premier, on en déduit que

— Soit p' divise p auquel cas $p' = p$ et dans ce cas $x \equiv 0[p]$ ce qui est impossible car $xyz \not\equiv 0[p]$.

— Soit p' divise y^{p-1} donc p' divise y. Par suite, p' divise $pgcd(x, y) = 1$. Absurde aussi.

$y + z$ et u sont des puissances p-iemes
$y + z$ et u sont premiers entre eux. Or, leur produit est une puissance $p-$ieme.
On écrit leur décomposition en facteurs premiers :

$$y + z = \prod_{p \in \mathcal{P}} q^{\alpha_k} \qquad u = \prod_{p \in \mathcal{P}} q^{\beta_k}$$

avec α_k et β_k non simultanément non nuls. Alors

$$(y + z)u = \prod_{p \in \mathcal{P}} q^{\alpha_k + \beta_k} = \prod_{q \in \mathcal{P}} q^{pc_k}$$

On en déduit que $p \mid \alpha_k + \beta_k$. Or, $\alpha_k \beta_k = 0$ donc $p \mid \alpha_k$ et $p \mid \beta_k$.

Donc chacun de ces deux facteurs est une puissance $p-$ieme : Il existe a, α tels que $y + z = a^p$ et $u = \alpha^p$. Par symétrie, on en déduit l'existence de b, c tels que $x + z = b^p$ et $x + y = c^p$.

3ème étape : q divise exactement l'un parmi x, y, z

Lemma 28.2. Si m est un entier non divisible par q alors $m^p \equiv \pm 1[q]$

— *Preuve du Lemme.* Par le petit théorème de Fermat, $m^{q-1} = m^{2p} \equiv 1[q]$. Or, q est premier donc $\mathbb{Z}/qZ$ est intègre. Par suite, l'équation $T^2 - 1 = (T-1)(T+1) = 0$ admet exactement deux solutions, ie $m^p \equiv \pm 1[q]$ □

Supposons que q ne divise pas xyz. Alors $x^p \equiv \pm 1, y^p \equiv \pm 1, z^p \equiv \pm 1[q]$ et donc la classe de $x^p + y^p + z^p$ modulo q est dans $\{\pm 3, \pm 1\}$. Or, $q = 2p + 1 \geq 5$ donc aucun n'est la classe de 0. Absurde.

Donc q divise l'un d'entre eux. Comme ils sont premiers entre eux, il divise exactement un seul d'entre eux. On peut supposer que q divise x et $yz \not\equiv 0[q]$.

4eme étape : q divise $y + z$ On rappelle $y + z = a^p$, $x + z = b^p$, $x + y = c^p$.

— Comme q divise x, il divise aussi $2x = b^p + c^p - a^p$.

— Comme $x \equiv 0[q]$, on en déduit que $y \equiv x + y \equiv c^p[q]$ Par ailleurs, q ne divise pas y, donc ne divise pas c et par le lemme $y \equiv \pm 1[q]$. De même, $z \equiv b^p \equiv \pm 1[q]$. Supposons que q ne divise pas $a = y + z$. Alors, $a^p \equiv \pm 1[q]$ et donc la classe de $b^p + c^p - a^p$ modulo q est dans $\{\pm 3, \pm 1\}$. C'est absurde car q divise $b^p + c^p - a^p$.

Donc q divise $y + z$.

Conclusion On a $y \equiv -z[q]$ donc

$$u = \sum_{k=0}^{p-1} (-z)^{p-1-k} y^k \equiv \sum_{k=0}^{p-1} y^{p-1} \equiv p y^{p-1}[q]$$

Or, $u = y^p + z^p = (-x)^p \equiv 0[q]$

Donc q divise py^{p-1}. Mais $q = 2p + 1$ ne peut pas diviser p. Donc q divise y^{p-1}. Or, $y \equiv \pm 1[q]$ et $p - 1$ est pair donc $y^{p-1} \equiv 1[q]$. Comme $q \neq 2$ c'est absurde. □

29 Structure des groupes abéliens finis

29.1 Recasages :

— 104 - Groupes finis. Exemples et applications.
— 120 - Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications.

29.2 Références :

— *NH2G2-2*, Caldero-Germoni [CG17b]
— *Rombaldi Algèbre*, [Rom17]
— *Gourdon Algèbre*, [Gou09]

29.3 Contexte

29.4 Prérequis

Definition 29.1. Soit G un GAF. On appelle *exposant* de G le maximum des ordres des éléments de G.

Lemma 29.2 ([Gou09])**.** Soit G un groupe abélien fini d'exposant r. Alors si $x \in G$, l'ordre de x divise r.

Remarque L'exposant de G est le PPCM des ordres des éléments de G.

Lemma 29.3 (Admis, cf [Rom17])**.** Soient $(n_k)_{1\leq k\leq r}$ et $(m_j)_{1\leq j\leq s}$ deux suites d'entiers tels que $n_{k-1} \mid n_k$ et $m_{j-1} \mid m_j$. Alors ces suites sont identiques ssi

$$\forall m \in \mathbb{N}^*, \prod_{k=1}^{r} m \wedge n_k = \prod_{j=1}^{s} m \wedge m_j$$

29.5 Développement

J'admets le lemme 29.3.

Virer l'unicité, et faire le lemme 29.2 à la place, c'est mieux pour la leçon groupes finis et l'unicité est un peu casse-gueule.

Theorem 29.4. Soit G un groupe abélien fini, et $H \subset G$ un sous-groupe. Alors tout caractère χ de H se prolonge en un caractère de G.

Démonstration. On adopte une notation multiplicative. G est abélien donc H est distingué. On fait une preuve par récurrence sur $[G : H]$ l'indice de H dans G.

— Si $[G : H] = 1$, alors $H = G$ donc la propriété est triviale.

— sinon supposons le résultat vrai pour tout sous-groupe K de G tel que $[G : H] > [G : K] \geq 1$.
Soit $x \in G$, $x \notin H$. Soit $\langle K, x\rangle$ le groupe engendré par H et x. Soit n le plus petit entier tel que $x^n \in H$ (existe car x est d'ordre fini et $1 \in H$). Remarquons que tout élément $z \in K$ s'écrit de façon unique comme $z = yx^k$ avec $y \in H$ et $k \in \{0, \ldots, n-1\}$.

Analyse : Supposons que l'on dispose d'un prolongement $\widetilde{\chi}$ de χ. Posons $\zeta := \chi(x)$. C'est une racine $n$ieme de 1. Alors pour $z = yx^k \in K$ on a

$$\widetilde{\chi}(z) = \chi(y)\zeta^k.$$

Synthèse : Soit ζ une racine nieme de l'unité. Pour $z = yx^k \in K$ on pose $\widetilde{\chi}(z) := \chi(y)\zeta^k$. Alors par unicité de la décomposition, $\widetilde{\chi}$ est bien défini. Montrons que c'est un morphisme de K dans $\mathbb{C}^*$: Considérons $h = yx^k$ et $h' = y'x^{k'}$ deux éléments de K.

— Si $0 \leq k + k' \leq n - 1$ alors

$$\widetilde{\chi}(hh') = \widetilde{\chi}(yy'x^{k+k'}) = \chi(y)\chi(y')\zeta^{k+k'} = \widetilde{\chi}(h)\widetilde{\chi}(h').$$

— Si $k + k' \geq n$ alors

$$\widetilde{\chi}(hh') = \widetilde{\chi}(yy'x^{k+k'-n}x^n) = \chi(y)\chi(y')\zeta^{k+k'-n}\chi(y)\chi(y')\zeta^{k+k'} = \widetilde{\chi}(h)\widetilde{\chi}(h').$$

Donc $\widetilde{\chi} \in \widehat{K}$ et prolonge χ. Or, $[G : K] = \dfrac{[G : H]}{[K : H]} < [G : H]$ car $[K : H] > 1$. Par l'hypothèse de récurrence, $\widetilde{\chi}$ se prolonge en $\widehat{\chi} \in \widehat{G}$, et ce prolongement est encore un prolongement de χ.

□

Theorem 29.5 (Structure des groupes abéliens finis)**.**
Soit G un GAF de cardinal au moins 2. Il existe une unique famille d'entiers $a_i \geq 2, i = 1, \ldots, s$, telle que

— $a_i \mid a_{i+1}$ pour $i = 1, \ldots, s-1$

— $G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \mathbb{Z}/a_s\mathbb{Z}$

Démonstration.

Existence :
On va raisonner par récurrence sur $|G|$:

— Si $|G| = 2$ alors $G \simeq \mathbb{Z}/2\mathbb{Z}$.

— Supposons que $|G| \geq 3$.

On trouve un "gros" facteur cyclique de G

Soit a l'exposant de G, et x un élément d'ordre maximal. Fixons ω une racine $a-$ième de l'unité et soit $\chi \in \widehat{\langle x \rangle}$ le caractère qui envoie x sur ω. χ est alors un isomorphisme $\langle x \rangle \simeq U_a$. D'après le théorème de relèvement, on peut prolonger χ en un morphisme $\widetilde{\chi}$ de G dans $\mathbb{C}^*$. Or, dans G l'ordre de tout élément divise a, et par suite l'image de $\widetilde{\chi}$ reste dans U_a. Posons $B := \operatorname{Ker} \widetilde{\chi}$. On a alors un isomorphisme

$$\varphi : \left\{ \begin{array}{ccc} B \times \langle x \rangle & \to & G \\ (h, x^k) & \mapsto & x^k h \end{array} \right.$$

En effet, puisque G est abélien, φ est bien un morphisme de groupes. De plus, si $(x^k, h) \in \operatorname{Ker} \varphi$ alors $x^k h = 1$ donc $\widetilde{\chi}(x^k h) = \chi(x)^k = \omega_a^k = 1$. Donc $a \mid k$. Puisque x est d'ordre a, alors $x^k = 1$ et par suite $h = 1$. Donc φ est injectif. Enfin pour la surjectivité, il suffit d'examiner le diagramme suivant et de remonter les flèches :

$$\begin{array}{ccc} G & \xrightarrow{\widetilde{\chi}} & U_a \\ \uparrow & \nearrow_{\chi} & \\ \langle x \rangle & & \end{array}$$

Soit $g \in G$. Posons $y := \chi^{-1}(\widetilde{\chi}(g)) \in \langle x \rangle$ et soit $h := y^{-1} g$. On vérifie alors que $h \in \operatorname{Ker} \widetilde{\chi}$, et alors $\varphi(h, y) = g$.
Donc

$$G \simeq B \times \mathbb{Z}/a\mathbb{Z}$$

avec a son exposant.

On applique l'hypothèse de récurrence à B

$|B| = \dfrac{|G|}{a} < |G|$ Donc par hypothèse de récurrence, il existe $a_1, \ldots, a_{s-1}$ tels que $a_i \mid a_{i+1}$ et $B \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \mathbb{Z}/a_{s-1}\mathbb{Z}$. Donc

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \mathbb{Z}/a_{s-1}\mathbb{Z} \times \mathbb{Z}/a\mathbb{Z}.$$

On pose $a_s := a$. Il suffit de vérifier que $a_{s-1} \mid a$, mais il existe un élément d'ordre a_{s-1} dans B, donc dans G et par suite $a_{s-1} \mid a_s$ puisque c'est l'exposant de G. D'où le résultat.

Unicité :

Supposons qu'il existe deux suites d'entiers $(a_1, \ldots, a_r)$ et $(b_1, \ldots, b_s)$ tel que

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \mathbb{Z}/a_r\mathbb{Z} \simeq \mathbb{Z}/b_1\mathbb{Z} \times \mathbb{Z}/b_s\mathbb{Z}$$

avec les conditions de divisibilités. Alors d'une part

$$\prod_{i=1}^{r} a_i = \prod_{j=1}^{s} b_j \tag{4.28}$$

D'autre part,

Si $r = 1$ alors $n := |G| = n_1$ est aussi l'exposant de G, mais cet exposant vaut m_s. Donc nécessairement $s = 1$ (sinon $n = m_1 \cdots m_s \geq 2m_s = 2n$).

Si $r \geq 2$ Alors $s \geq 2$. Soit $m \in \mathbb{N}^*$. Par le morphisme de translation par m, $x \mapsto mx$, on a donc

$$\prod_{i=1}^{r} m\mathbb{Z}/a_i\mathbb{Z} \simeq \prod_{j=1}^{s} m\mathbb{Z}/b_j Z$$

Or, $|m\mathbb{Z}/a_i\mathbb{Z}| = \dfrac{a_i}{m \wedge a_i}$ et par suite on a l'égalité

$$\prod_{i=1}^{r} \frac{a_i}{m \wedge a_i} = \prod_{j=1}^{s} \frac{b_j}{m \wedge b_j} \tag{4.29}$$

Par (4.28) et (4.29) on déduit que

$$\prod_{i=1}^{r} m \wedge a_i = \prod_{j=1}^{s} m \wedge b_j$$

L'unicité tombe alors du lemme 29.3 □

30 [WARNING] Suite de Polygones et déterminant circulant

30.1 Recasages :

— 152 - Déterminant. Exemples et applications.

— 182 - Applications des nombres complexes à la géométrie.

30.2 Référence

Gourdon Algèbre [Gou09] pour le calcul du déterminant. Sans référence pour le reste.

30.3 Développement

Theorem 30.1. Soit $(a_0, \dots, a_{n-1})$ des complexes et soit $P := \sum_{i=0}^{n-1} a_i X^i$ le polynôme associé. Posons $\omega := e^{2i\pi/n}$ une racine $n$ieme de l'unité. Alors

$$\begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ a_1 & \dots & a_{n-1} & a_0 \end{vmatrix} = \prod_{k=0}^{n-1} P(\omega^k)$$

Theorem 30.2. Soit $P := (M_1, \dots, M_n)$ un polygone convexe du plan. On définit par récurrence une suite de polygones (P_k) avec $P_0 = P$ et les sommets de P_{k+1} sont les milieux des arêtes de P_k. Alors (P_k) converge vers l'isobarycentre de P.

30.4 Déterminant circulant

Démonstration. On pose $A := \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ a_1 & \dots & a_{n-1} & a_0 \end{pmatrix}$ et $J := \begin{pmatrix} 0 & 1 & (0) & \\ \vdots & \ddots & \ddots & \\ 0 & & \ddots & 1 \\ 1 & 0 & \dots & 0 \end{pmatrix}$

En évaluant sur la base canonique de $\mathbb{C}^n$, on a que $J^p = \begin{pmatrix} 0 & I_{n-p} \\ I_p & 0 \end{pmatrix}$

On en déduit que pour tout $\alpha_0, \dots, \alpha_{n-1} \in \mathbb{C}$,

$$\sum_{i=0}^{n-1} \alpha_i J^i = \begin{pmatrix} \alpha_0 & \alpha_1 & \dots & \alpha_{n-1} \\ \alpha_{n-1} & \alpha_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \alpha_1 \\ \alpha_1 & \dots & \alpha_{n-1} & \alpha_0 \end{pmatrix}$$

On en déduit que $A = P(J)$, $J^n = I_n$ et si Q est un polynôme non nul de degré $\deg Q < n$ alors $Q(J) \neq 0$. Donc, $X^n - 1$ est le polynôme minimal de J. Puisqu'il est scindé à racines simples, on en déduit que J est diagonalisable, et ses valeurs propres sont les ω_k.

Par suite, dans une base de diagonalisation,

$$J \simeq \begin{pmatrix} 1 & & & \\ & \omega & & (0) \\ & & \ddots & \\ & (0) & & \omega^{n-1} \end{pmatrix}$$

Par suite,

$$A = P(J) \simeq \begin{pmatrix} P(1) & & & \\ & P(\omega) & & (0) \\ & & \ddots & \\ & (0) & & P(\omega^{n-1}) \end{pmatrix}$$

Et donc puisque le déterminant est un invariant de similitude,

$$\det A = P(1)P(\omega)\cdots P(\omega^{n-1})$$

□

30.5 Suite de polygones

Démonstration.

Insérer un dessin

On va utiliser les complexes pour résoudre ce problème de géométrie. On identifie le plan euclidien au plan complexe et on note $(z_1, \dots, z_n) \in \mathbb{C}^n$ les affixes de $M_1, \dots, M_n$. Alors, P_k est représenté par le tuple $Z_k := (z_1^{(k)}, \dots, z_n^{(k)})$ avec $z_i^{(0)} := z_i$ et

$$z_i^{(k+1)} = \frac{z_i^{(k)} + z_{i+1}^{(k)}}{2}$$

les indices étant pris modulo n. La suite Z_k vérifie donc l'hypothèse de récurrence

$$Z_{k+1} = AZ_k \text{ avec } A = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 0 & \dots & 0 \\ 0 & \frac{1}{2} & \frac{1}{2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 0 & \dots & 0 & \frac{1}{2} \end{pmatrix}$$

Calculons son polynôme caractéristique :

$$\chi_A = \det(XIn - A) = \begin{vmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_1 \\ a_1 & \dots & a_{n-1} & a_0 \end{vmatrix}$$

avec $a_0 = X - \frac{1}{2}$, $a_1 = -\frac{1}{2}$ et $a_i = 0$ pour $i > 2$. On reconnaît là un *Déterminant Circulant.*

En posant $\omega := e^{2i\pi/n}$ et $P(T) := \left(X - \frac{1}{2}\right) - \frac{1}{2}T \in (\mathbb{C}[X])[T]$

on a donc

$$\chi_A = P(1)P(\omega)\cdots P(\omega^{n-1}) = \prod_{k=0}^{n-1}\left(X - \frac{1}{2} - \frac{1}{2}\omega^k\right) = \prod_{k=0}^{n-1}\left(X - \left(\frac{1+\omega^k}{2}\right)\right) \in \mathbb{C}[X]$$

χ_A est scindé à racines simples, donc A est diagonalisable et ses valeurs propres sont les $\lambda_k := \dfrac{1+\omega^k}{2}$: Il existe $P \in GL_n(\mathbb{R})$ telle que

$$A = P \begin{pmatrix} 1 & & & \\ & \lambda_1 & & \\ & & \ddots & \\ & & & \lambda_{n-1} \end{pmatrix} P^{-1}$$

Or pour $k \geq 1$,

$$|\lambda_k| = \left|\cos\left(\frac{k\pi}{n}\right)\right| < 1$$

On en déduit que

$$A^k \to P \begin{pmatrix} 1 & & & \\ & 0 & & \\ & & \ddots & \\ & & & 0 \end{pmatrix} P^{-1} =: B$$

Par suite, $Z_k = A^k Z \to BZ$.

Ainsi, d'une part $AZ_k \to A(BZ)$ par continuité, d'autre part $AZ_k = A^{k+1}Z \to BZ$ Donc par unicité de la limite, $A(BZ) = BZ$, ie BZ est un vecteur propre de A associé à la valeur prore 1. Puisque cet espace propre est de dimension 1 et qu'il contient $\begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}$ (La somme des lignes de A est constante à 1) on en déduit que BZ est de la forme $\begin{pmatrix} z \\ \vdots \\ z \end{pmatrix}$

C'est à dire que la suite de polygones P_k converge vers le point d'affixe z.

Soit G_k le barycentre de P_k. On note g_k son affixe.

Alors

$$g_{k+1} = \frac{1}{n}\sum_{i=1}^{n} z_i^{(k+1)} = \frac{1}{n}\sum_{i=1}^{n} \frac{z_i^{(k)} + z_{i+1}^{(k)}}{2} = \frac{1}{n}\sum_{i=1}^{n} z_i^{(k)} = g_k$$

Donc G_k est constante, à $G_0 = G$ d'affixe g l'isobarycentre de P. Par continuité, on en déduit que $g = z$, d'où le résultat. □

31 Théorème d'Abel Angulaire et Taubérien Faible

31.1 Références :

— *40 développements d'Analyse*, J et L Bernis [Ber18]

31.2 Théorème d'Abel Angulaire

Theorem 31.1. Soit $\sum a_n z^n$ une série entière de rayon de convergence supérieur ou égal à 1, et de somme f. Soit $\theta_0 \in [0, \frac{\pi}{2}[$. On s'intéresse au domaine angulaire suivant :

$$A_{\theta_0} = \{1 - \rho \exp(i\theta), \theta \in [-\theta_0, \theta_0], \rho \in \mathbb{R}_+^*\} \cap D(0,1)$$

Alors si la série $\sum a_n$ converge, alors

$$\lim_{z \to 1, z \in A_{\theta_0}} f(z) = \sum_{n=0}^{+\infty} a_n$$

Démonstration.

Insérer un dessin ici, ça sera plus clair

Transformation d'Abel Supposons que la série converge. Notons $S := \sum_{n=0}^{+\infty} a_n$ sa somme, que $S_n := \sum_{k=0}^{n} a_k$ sa somme partielle et $R_n := \sum_{k=n+1}^{+\infty} a_k$ son reste d'ordre n. Alors pour tout $n \in \mathbb{N}^*$ on a $a_n = R_{n-1} - R_n$. Soit $N \in \mathbb{N}^*$ et $|z| < 1$.

$$\begin{aligned}\sum_{n=0}^{N} a_n z^n - S_N &= \sum_{n=1}^{N} a_n(z^n-1)\\ &= \sum_{n=1}^{N} (R_{n-1}-R_n)(z^n-1)\\ &= \sum_{n=0}^{N-1} R_n(z^{n+1}-1) - \sum_{n=1}^{N} R_n(z^n-1)\\ &= \sum_{n=0}^{N-1} R_n(z^{n+1}-1) - \sum_{n=0}^{N} R_n(z^n-1)\\ &= \sum_{n=0}^{N} R_n(z^{n+1}-z^n) - R_N(z^{N+1}-1)\\ &= (z-1)\sum_{n=0}^{N} R_n z^n - R_N(z^{N+1}-1)\end{aligned}$$

Or, $|R_N(z^{N+1}-1)| \leq 2|R_N| \to 0$. Comme le membre de gauche converge, en en déduit que le membre de droite aussi et en passant à la limite on obtient

$$f(z) - S = (z-1)\sum_{n=0}^{+\infty} R_n z^n$$

Soit $\varepsilon > 0$. Par convergence de la série $\sum a_n$ on dispose de n_0 tel que pour $n \geq n_0, |R_n| \leq \varepsilon$.

Ainsi, par inégalité triangulaire,

$$\begin{aligned}|f(z) - S| &\leq |z-1|\left|\sum_{n=0}^{n_0} R_n z^n\right| + \varepsilon|z-1|\sum_{n=n_0+1}^{+\infty}|z|^n\\ &\leq |z-1|\sum_{n=0}^{n_0}|R_n| + \varepsilon\frac{|z-1|}{1-|z|}\end{aligned}$$

Et cette inégalité est vraie pour tout z de module strictement inférieur à 1.

Posons $\eta := \dfrac{\varepsilon}{\sum_{n=0}^{n_0}|R_n|+1}$

Soit z dans le disque vérifiant $|z-1| < \eta$.

Alors

$$|f(z) - S| \leq \varepsilon + \varepsilon\frac{|z-1|}{1-|z|}$$

Supposons de plus que $z \in A_{\theta_0}$. Alors par définition on dispose de $\rho \in \mathbb{R}_+^*$ et $\theta \in [-\theta_0, \theta_0]$ tel que $z = 1 - \rho\exp(i\theta)$

En particulier

$$|z|^2 = 1 + \rho^2 - 2\rho\cos(\theta)$$

et donc

$$\frac{|z-1|}{1-|z|} = \frac{|z-1|(1+|z|)}{1-|z|^2} \leq \frac{2\rho}{2\rho\cos(\theta)-\rho^2} \leq \frac{2}{2\cos(\theta)-\rho}$$

Supposons de plus que z est tel que $\rho := |z-1| < \cos(\theta_0)$. C'est possible car $\theta_0 \neq \frac{\pi}{2}$ et donc $\cos(\theta_0) \neq 0$.

Alors, comme de plus $\theta \in]-\theta_0, \theta_0[\subset]-\frac{\pi}{2}, \frac{pi}{2}[$ on en déduit que $\cos(\theta) \geq \cos(\theta_0)$.

Par suite,

$$\frac{|z-1|}{1-|z|} \leq \frac{2}{2\cos(\theta_0)-\cos(\theta_0)} \leq \frac{2}{\cos(\theta_0)}$$

Et donc pour $|z-1| < \min\{\eta, \cos(\theta_0)\}$ on a

$$|f(z)-S| \leq \varepsilon\left(1+\frac{2}{\cos(\theta_0)}\right)$$

□

31.3 Application du théorème de convergence angulaire

On va se placer dans le cas simplifié où la convergence est radiale.

Soient $\sum a_n, \sum b_n$ deux séries convergentes. Notons $\sum c_n$ la série produit de Cauchy de ces deux séries. Si la série $\sum c_n$ converge, alors

$$\sum_{n=0}^{+\infty} c_n = \sum_{n=0}^{+\infty} a_n \sum_{n=0}^{+\infty} b_n$$

En effet, la convergence des série $\sum a_n$ et $\sum b_n$ donne que les séries entières associées ont un rayon de convergence au moins 1. Par produit de Cauchy de deux séries entières, on en déduit que la série entière $\sum c_n z^n$ a aussi un rayon de convergence au moins 1 et pour tout $t \in]-1,1[$,

$$\sum_{n=1}^{+\infty} c_n t^n = \sum_{n=1}^{+\infty} a_n t^n \sum_{n=1}^{+\infty} b_n t^n =$$

En faisant tendre $t \to 1$ par valeur inférieur, on en déduit le résultat en appliquant le théorème d'Abel.

31.4 Théorème Taubérien Faible

Sorte de réciproque

Theorem 31.2. Soit $\sum a_n z^n$ une série entière de rayon de convergence égal à 1. On note f sa somme sur $\{|z|<1\}$. Supposons qu'il existe $S \in \mathbb{C}$ tel que $\lim\limits_{x \to 1^-} f(x) = S$.

Alors, si $a_n = o(1/n)$, la série $\sum a_n$ converge et on a

$$S = \sum_{n=0}^{+\infty} a_n$$

Démonstration. Pour tout $N \in \mathbb{N}^*$ posons $S_N := \sum_{n=0}^{N} a_n$ la somme partielle. Alors pour $x \in]0,1[$,

$$S_N - f(x) = \sum_{n=0}^{N} a_n(1-x^n) - \sum_{n=N+1}^{+\infty} a_n x^n$$

Or,

— D'une part, pour tout $x \in]0,1[$, et pour tout $n \in \mathbb{N}^*$,

$$1 - x^n = (1-x)(1 + x + \cdots + x^{n-1}) \leq n(1-x)$$

— D'autre part, $na_n = o(x^n)$ donc par comparaison de séries à termes positifs, $\sum_{n \geq N+1} \frac{n}{N}|a_n|x^n$ est une série convergente. Par suite,

$$\left| \sum_{n=N+1}^{+\infty} a_n x^n \right| \leq \sum_{n=N+1}^{+\infty} \frac{n}{N}|a_n|x^n \leq \sup(n|a_n|)\frac{1}{N(1-x)}$$

Alors pour $x \in]0,1[$:

$$|S_N - f(x)| \leq (1-x)\sum_{n=0}^{N} n|a_n| + \sup_{n>N}(n|a_n|)\frac{1}{N(1-x)}$$

Posons $x := 1 - \frac{1}{N}$
Alors

$$\left| S_N - f\left(1 - \frac{1}{N}\right) \right| \leq \frac{1}{N}\sum_{n=0}^{N} n|a_n| + \sup_{n>N}(n|a_n|)$$

Or, $\sup(n|a_n|) \to 0$, et par le *Théorème de Césaro*, $\frac{1}{N}\sum_{n=0}^{N} n|a_n| \to 0$
Finalement,

$$|S_N - S| \leq \left| S_N - f\left(1 - \frac{1}{N}\right) \right| + \left| f\left(1 - \frac{1}{N}\right) - S \right| \to 0$$

□

32 [WARNING] Suites équiréparties : Critère de Weyl

Référence : FGN *Analyse 2* [FN07c]

32.1 Développement

Theorem 32.1. Soit u_n une suite de $[0,1]$. Pour tout $0 \leq a \leq b \leq 1$, on pose

$$X_n(a,b) := Card\{k \in [\![n,p]\!] \mid u_k \in [a,b]\}$$

Alors s'équivalent :

i $\dfrac{X_n(a,b)}{n} \to b-a$ pour tout couple (a,b)

ii Pour toute fonction $f : [0,1] \to \mathbb{R}$ continue on a :

$$\lim_{n\to\infty} \sum_{k=1}^{n} f(u_k) = \int_0^1 f(t)dt$$

iii Pour tout $p \in \mathbb{N}^*$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{k=1}^{n} e^{2i\pi p u_k} = 0$$

32.2 Preuve

Démonstration.

$(i \Rightarrow ii)$ $X_n(a,b) = \dfrac{1}{n}\sum_{k=1}^{n} \mathbb{1}_{[a,b]}(u_k)$ et $\int_0^1 \mathbb{1}_{[a,b]} = b-a$ donc (i) donne que pout tout segment S de $[0,1]$,

$$\frac{1}{n}\sum_{k=1}^{n} \mathbb{1}_S(u_k) \to \int_0^1 \mathbb{1}_S(t)dt$$

.

Par linéarité c'est aussi vrai pour les fonctions en escalier. Soit f une fonction continue. Soit $\varepsilon > 0$. Par densité des fonctions en escalier, il existe g en escalier telle que $\|f-g\|_\infty \leq \dfrac{\varepsilon}{3}$.

Alors,

$$\begin{aligned}\left|\frac{1}{n}\sum_{k=1}^{n} f(u_k) - \int_0^1 f(t)dt\right| &\leq \left|\frac{1}{n}\sum_{k=1}^{n} f(u_k) - \frac{1}{n}\sum_{k=1}^{n} g(u_k)\right| \\ &+ \left|\frac{1}{n}\sum_{k=1}^{n} g(u_k) - \int_0^1 g(t)dt\right| \\ &+ \left|\int_0^1 g(t)dt - \int_0^1 f(t)dt\right| \\ &\leq \|f-g\|_\infty + \left|\frac{1}{n}\sum_{k=1}^{n} g(u_k) - \int_0^1 g(t)dt\right| + \|f-g\|_\infty\end{aligned}$$

Or, g est en escalier, donc $\left|\frac{1}{n}\sum_{k=1}^{n} g(u_k) - \int_0^1 g(t)dt\right| \to 0$ et par suite il existe N tel que pour $n \geq N$,

$$\left|\frac{1}{n}\sum_{k=1}^{n} f(u_k) - \int_0^1 f(t)dt\right| \leq \varepsilon$$

($ii \Rightarrow i$) Soit $I = [a,b] \subset [0,1]$. On va encadrer $\mathbb{1}_I$ par deux fonctions continues :

— On définit ψ_k nulle sur $[0,a]$ et $[b,1]$, vaut 1 sur $[a+\frac{1}{k}, b-\frac{1}{k}]$ et affine sur $[a, a+\frac{1}{k}]$ et $[b-\frac{1}{k}, b]$.

— Pour k assez grand, φ_k est nulle sur $[0, a-\frac{1}{k}]$ et $[b+\frac{1}{k}, 1]$ (ces intervalles étant éventuellement vides si $a=0$ ou $b=1$), vaut 1 sur $[a,b]$ et est affine sur $[a-\frac{1}{k}, a]$, $[b, b+\frac{1}{k}]$.

Alors, pour p assez grand, ψ_p, φ_p sont continues et

$$\psi_p \leq \mathbb{1}_I \leq \varphi p$$

Par suite,

$$\frac{1}{n}\sum_{k=1}^{n} \psi_p(u_k) \leq \frac{X_n(a,b)}{n} \leq \frac{1}{n}\sum_{k=1}^{n} \varphi_p(u_k)$$

Or,

$$\begin{cases} \frac{1}{n}\sum_{k=1}^{n} \psi_p(u_k) & \to & \int_0^1 \psi_p(t)dt = b-a-\frac{1}{p} \\ \frac{1}{n}\sum_{k=1}^{n} \phi_p(u_k) & \to & \int_0^1 \varphi_p(t)dt = b-a+\frac{1}{p} \end{cases}$$

Soit $\varepsilon > 0$, et soit p tel que $\frac{1}{p} \leq \frac{\varepsilon}{2}$. Alors :

$$\begin{aligned}\left|\frac{1}{n}\sum_{k=1}^{n}\psi_p(u_k)-(b-a)\right| &= \left|\frac{1}{n}\sum_{k=1}^{n}\psi_p(u_k)-(b-a-\frac{1}{p})-\frac{1}{p}\right| \\ &\leq \frac{\varepsilon}{2}+\frac{1}{p} \\ &\leq \frac{\varepsilon}{2}+\frac{\varepsilon}{2} \\ &\leq \varepsilon\end{aligned}$$

Pour n assez grand.

De même,

$$\left|\frac{1}{n}\sum_{k=1}^{n}\phi_p(u_k)-(b-a)\right| \leq \varepsilon$$

pour n assez grand, et donc il existe N tel que pour $n \geq N$,

$$\left|\frac{X_n(a,b)}{n}-(b-a)\right| \leq \varepsilon$$

(*ii* $\Rightarrow$ *iii*) Il suffit de décomposer selon les parties réelle et imaginaire :

$$\begin{aligned}\frac{1}{n}\sum_{k=1}^{n}e^{2i\pi p u_k} &= \frac{1}{n}\sum_{k=1}^{n}\cos(2i\pi p u_k)+i\frac{1}{n}\sum_{k=1}^{n}\sin(2i\pi p u_k) \\ &\to \int_0^1\cos(2\pi pt)dt+i\int_0^1\sin(2\pi pt)dt=0\end{aligned}$$

(*iii* $\Rightarrow$ *ii*) Par linéarité, ce résultat est vrai pour tout polynôme trigonométrique. Or, toute fonction continue vérifiant $f(0)=f(1)$ est limite uniforme de polynômes trigonométriques. Donc le résultat est vrai pour toute fonction continue.

Si maintenant f est continue et ne vérifie pas $f(0)=f(1)$ posons $g:=f$ sur $[\varepsilon,1]$, $g(0)=g(1)=f(1)$ et g affine sur $[0,\varepsilon]$. Alors

$$\int_0^1|f-g|=\int_0^\varepsilon|f-g|(t)dt \leq \|f-g\|_\infty\varepsilon$$

□

33 Théorème des extrema liés et sous-variétés [Timé]

33.1 Remarques sur le timing

En fait ce dev va très bien en 15 min avec l'application. Il ne faut pas être ambitieux, il y a plusieurs choses à dire, à écrire. C'est intéressant de faire un schéma pour expliquer l'interprétation géométrique derrière ce résultat.

Partie présentée : Théorème des extrema liés : M est une sous variété de $\mathbb{R}^n$ en explicitant la submersion, en insistant sur le rang de $dg(x)$. Puis $df(x)$ est nulle sur l'espace tangent. 3eme colonne : Partie dualité et orthogonalité pour avoir l'existence des λ_i. L'unicité vient de la liberté de la famille $(dg_i(x))$. 4eme colonne : Application au théorème spectral.

Timing : 15'47, je peux aller plus vite en réalité.

33.2 Recasages :

- 151 - Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications.
- 159 - Formes linéaires et dualité en dimension finie. Exemples et applications.
- 214 - Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.
- 219 - Extremums : Existence, caractérisation, recherche. Exemples et applications.

33.3 Références :

- *Calcul Différentiel*, Avez [Ave97] pour la preuve
- *Introduction aux variétés différentielles*, Lafontaine [Laf97] pour les théorèmes utiles
- Rouvière [Rou03] pour l'intuition géométrique

Faire un dessin de sous-variété ?

33.4 Prérequis

Definition 33.1. Soit U un ouvert de $\mathbb{R}^n$ et $g : U \mapsto \mathbb{R}^p$ une application de classe $\mathcal{C}^k$.

- On dit que g est une *submersion* de classe $\mathcal{C}^k$ ssi pour tout $a \in U, dg(a)$ est *surjective*.
- On dit que g est une *immersion* de classe $\mathcal{C}^k$ ssi pour tout $a \in U, dg(a)$ est *injective*.

Theorem 33.2 (Submersion)**.** Soit U un ouvert de $\mathbb{R}^q$ contenant 0 et

$$f : U \to \mathbb{R}^p$$

une application $\mathcal{C}^1$. On suppose que $df(0)$ est surjective (ie que f est une submersion en 0). Alors il existe un ouvert W de $\mathbb{R}^p$ et un $\mathcal{C}^1$ difféomorphisme $\varphi : W \to \varphi(W)$ tel que $0 \in \varphi(W) \subset U$ et

$$f(\varphi(x_1, \ldots, x_q)) = (x_1, \ldots, x_p)$$

Démonstration. On constate que $p \leq q$ car la différentielle est surjective, donc de rang p. Alors il existe une matrice extraite inversible de la Jacobienne de taille p.

Quitte à faire un changement de base, on peut donc supposer que la jacobienne de $f = (f_1, \ldots, f_p)$ en 0 a pour forme

$$df(0) = \begin{pmatrix} A & \star \\ \star & \star \end{pmatrix}, \quad A \in GL_p(\mathbb{R})$$

.

Posons alors la fonction h comme suit où $\pi_i(x)$ est la $i - ime$ coordonnée de x :

$$h(x) = (f_1(x), \ldots, f_p(x), \pi_{p+1}(x), \pi_q(x))$$

La différentielle de h en zéro s'écrit alors

$$dh(0) = \begin{pmatrix} A & \star \\ 0 & I_{p-q} \end{pmatrix}, \quad A \in GL_p(\mathbb{R})$$

.

Ainsi, $dh(0)$ est inversible, donc par le *Théorème d'inversion locale*, h est un $\mathcal{C}^1$ difféomorphisme d'un voisinage V de 0 vers $W := h(V)$. On pose $\varphi = h^{-1}$. Alors

$$h(\varphi(x)) = x$$

et

$$h(u) = (f(u), u_{p+1}, \ldots, u_q)$$

donc pour x dans le voisinage W on a

$$f(\varphi(x)) = (x_1, \ldots, x_p)$$

□

Definition 33.3. Une partie M de $\mathbb{R}^n$ est une sous-variété de $\mathbb{R}^n$ de dimension p (ou de codimension $n - p$) si pour tout point $x \in M$ il existe des voisinages ouverts U de x et V de 0 dans $\mathbb{R}^n$ et un $\mathcal{C}^1$ difféomorphisme φ de U sur $V = \varphi(U)$ vérifiant

$$\varphi(U \cap M) = V \cap (\mathbb{R}^p \times \{0\})$$

Exemples

— Le cercle unité S^1 est une sous-variété de dimension 1 de $\mathbb{R}^2$.

— Tout sous-espace affine de dimension d est une sous-variété de dimension d

— Si $p = n$ alors $\varphi(U \cap M) = \varphi(U) \cap \mathbb{R}^n = \varphi(U)$ et donc $U \cap M = U$. Par suite $M = U$ est un ouvert de $\mathbb{R}^n$. Les sous variétés de $\mathbb{R}^n$ de dimension n sont donc des ouverts de $\mathbb{R}^n$. La réciproque est aussi vraie.

— si $p = 0$ alors $\mathbb{R}^p = \{0\}$ et $\varphi(U \cap M) = \{0\}$. Donc $U \cap M = \{\varphi^{-1}(0)\}$. Les sous variétés de dimension 0 sont des parties discrètes. Et réciproquement.

Remark 33.4. La notion de sous-variété permet de voir certaines parties de $\mathbb{R}^n$ localement comme des parties de $\mathbb{R}^p$ et possèdent en particulier localement les même propriétés topologiques.

Il existe plusieurs définitions équivalentes de la notion de sous-variété. Tout est condensé dans le théorème suivant

Theorem 33.5 (Des Sous-variétés)**.** Soit M une partie de $\mathbb{R}^n$. Les propriétés suivantes sont équivalentes :

(i) M est une sous variété de $\mathbb{R}^n$ de dimension p

(ii) *[Implicite]* Pour tout a de M, il existe un ouvert U de $\mathbb{R}^n$ contenant a et une submersion $g : U \to \mathbb{R}^{n-p}$ telle que $U \cap M = g^{-1}(0)$

(iii) *[Paramétrique]* Pour tout a de M, il existe un ouvert U de $\mathbb{R}^n$ contenant a, un ouvert Ω de $\mathbb{R}^p$ contenant 0, une application $h : \Omega \to \mathbb{R}^n$ qui est à la fois une immersion dans $\mathbb{R}^n$ et un homéomorphisme de Ω sur $U \cap M$.

(iv) *[Graphe]* Pour tout a de M, il existe un ouvert U de $\mathbb{R}^n$ contenant a, un ouvert V de $\mathbb{R}^p$ contenant $(a^1, \dots, a^p)$ et une application $\mathcal{C}^1$ G de V dans $\mathbb{R}^{n-p}$ tels que, après permutation éventuelle des coordonnées, $U \cap M$ soit égal au graphe de G : En notant $G = (g_1, \dots, g_{n-p})$ on a donc

$$(x \in M \cap U) \Leftrightarrow \begin{cases} (x_1, \dots, x_p) \in V \\ x_{p+1} = g_1(x_1, \dots, x_p), \dots, x_n = g_{n-p}(x_1, \dots, x_p) \end{cases}$$

Remarques On a donné toutes les implications pour pouvoir répondre aux questions du Jury si besoin mais on ne va avoir besoin que du point facile $(i) \Leftrightarrow (ii)$ qui donne la caractérisation suivante :

Theorem 33.6. Soit g une application $\mathcal{C}^1$ d'un ouvert U de $\mathbb{R}^n$ dans $\mathbb{R}^p$, et soit $a \in \mathbb{R}^p$ tel que $M := g^{-1}(a) \neq \emptyset$. Alors pour que M soit une sous variété il suffit que la différentielle de g soit surjective en tout point de M.

Avant de faire la preuve de ce point, donnons quelques éléments de preuve pour le reste (voir [Laf97] pour les preuves plus précises, [Rou03] pour avoir des idées).

— L'implication $(ii) \Rightarrow (iv)$ résulte du *Théorème des fonctions implicites* en résolvant le système d'équations $f_1(x) = \dots = f_{n-p}(x) = 0$ par rapport à $x_{p+1}, \dots, x_n$.

— L'implication (iii) ⇒ (iv) résulte du *Théorème d'inversion locale*. En effet, en écrivant

$$h : (u_1, \dots, u_p) \mapsto x = (h_1(u), \dots, h_p(u))$$

On inverse $(h_1, \dots, h_p)$ pour obtenir $u_1, \dots, u_p$ en fonction de $x_1, \dots, x_p$ que l'on reporte ensuite dans $h_{p+1}, \dots, h_n$ pour avoir $x_{p+1}, \dots, x_n$ en fonction de $x_1, \dots, x_p$.

— Le théorème de la submersion 33.2 admet un théorème dual dit théorème de l'immersion 33.2 qui se prouve essentiellement de la même façon.

Theorem 33.7 (de l'immersion)**.** Soit f une application $\mathcal{C}^1$ d'un ouvert U de $\mathbb{R}^p$ dans $\mathbb{R}^q$. On suppose que $0 \in U$ et que la différentielle $df(0)$ est injective (ie f est une immersion en 0). Alors il existe un ouvert V de $\mathbb{R}^p$, un ouvert U' tel que $0 \in U' \subset U$ et $f(U') \subset V$ et un difféomorphisme φ de V sur son image tel que

$$\varphi(f(x_1, \dots, x_p)) = f(x_1, \dots, x_p, 0, \dots, 0)$$

Démonstration. On remarque que $p \leq q$ puisque $df(0) : \mathbb{R}^p \to \mathbb{R}^q$ est injective.
Soit $f_1, \dots, f_q$ les composantes de f. Comme f est une immersion en 0 la jacobienne $df(0)$ est de rang p et donc il existe une matrice extraite inversible de taille p. Quitte à permuter les coordonnées on peut donc supposer que la matrice jacobienne a une forme

$$\begin{pmatrix} A & \star \\ \star & \star \end{pmatrix}, \quad A \in GL_p(\mathbb{R})$$

On définit alors une application $g : U \times \mathbb{R}^{q-p} \to \mathbb{R}^q$ en posant

$$g(x_1, \dots, x_p, y_1, \dots, y_{q-p}) = (f_1(x), \dots, f_p(x), y_1 + f_{p+1}(x), \dots, y_{q-p} + f_q(x))$$

Alors,

$$dg(0) = \begin{pmatrix} A & 0 \\ \star & I_{q-p} \end{pmatrix}$$

est inversible. Par le *Théorème d'Inversion Locale* il existe un ouvert W contenant 0 tel que g soit un $\mathcal{C}^1-$difféomorphisme de W vers $V := g(W)$. On pose $\varphi = g^{-1}$ qui convient. □

Preuve du théorème des sous variétés

Démonstration.

Sens facile (*i*) ⇒ (*ii*) Soit f le difféomorphisme défini sur un voisinage U de $a \in M$, donné par (i), et considérons les composantes (f^i) de f. Puisque f est un difféomorphisme, les différentielles des f^i sont linéairement indépendantes en tout point de U. Posons

$$g = (f^{p+1}, \dots, f^n).$$

Alors g est une submersion de U dans $\mathbb{R}^{n-p}$ telle que $M \cap U = g^{-1}(\{0\})$. D'où (ii).

$(ii) \Rightarrow (i)$ On va utiliser le théorème de la submersion 33.2 Soit $a \in M$, U_a un voisinage ouvert de a et $g_a : U_a \to \mathbb{R}^{n-p}$ une submersion telle que $U_a \cap M = g_a^{-1}(\{0\})$. Alors par le théorème de la submersion (33.2), il existe un voisinage ouvert W_a et un $\mathcal{C}^1-$diffeomorphisme φ tels que

$$g_a(\varphi(x_1, \ldots, x_n)) = (x_{p+1}, \ldots, x_n)$$

Alors

$$\varphi^{-1}(U_a \cap M) = \varphi^{-1}(g_a^{-1}(\{0\})) = (g_a \circ \varphi)^{-1}(\{0\}^{n-p}) = W_a \cap (\mathbb{R}^p \times \{0\}^{n-p})$$

donc M est une sous variété, de dimension p. □

Definition 33.8. On dit qu'un vecteur v est tangent en un point a d'une partie A de $\mathbb{R}^p$ s'il existe $\varepsilon > 0$ et une application dérivable $\gamma :]-\varepsilon, \varepsilon[\to \mathbb{R}^p$ telle que $\gamma(]-\varepsilon, \varepsilon[) \subset A$, $\gamma(0) = a, \gamma'(0) = v$.

Theorem 33.9. Les vecteurs tangents en un point à une sous-variété de dimension p de $\mathbb{R}^n$ forment un espace vectoriel de dimension p. L'espace des vecteurs tangents à une sous-variété M en un point x est noté T_xM et est appelé *Espace Tangent*.

Démonstration. Soit $x \in M$. Soit (U, f) une carte locale (ie un voisinage ouvert de x, V un voisinage ouvert de 0 et $f : U \to V$ un $\mathcal{C}^1$difféomorphisme redressant M) :

$$f(U \cap M) = f(U) \cap \left(\mathbb{R}^p \times \{0\}^{n-p}\right).$$

Prouvons que

$$T_X M = df(0)^{-1}\left(\mathbb{R}^p \times \{0\}^{n-p}\right)$$

Soit v tangent en x, et soit γ tracé sur M tel que $\gamma(0) = x$ et $\gamma'(0) = v$. Quitte à restreindre l'intervalle de définition on peut supposer que $\gamma(]-\varepsilon, \varepsilon[) \subset U \cap M$. Alors par composition

$$df(0) \cdot v \in \mathbb{R}^p \times \{0\}^{n-p}$$

ie

$$v \in df(0)^{-1}\left(\mathbb{R}^p \times \{0\}^{n-p}\right).$$

Réciproquement, soit $w \in \mathbb{R}^p \times \{0\}^{n-p}$ et choisissons ε de sorte que

$$\forall |t| < \varepsilon, tw \in f(U).$$

Posons alors $\gamma(t) := f^{-1}(tw)$. γ est donc un arc $\mathcal{C}^1$ tracé sur M, $\gamma(0) = f^{-1}(0) = x$ et $\gamma'(0) = df(0)^{-1} \cdot w$ est tangent à M en x.

Donc T_xM est un espace vectoriel, et puisque $df(0)$ est un isomorphisme, $\dim T_xM = p$ □

Remarque

— Si M est une sous-variété et si g est une submersion définie sur un voisinage U de a et telle que $U \cap M = g^{-1}(g(a))$ alors $T_aM = \ker dg(a)$.

— Si M est définie au voisinage de a par une paramétrisation (ie une application g d'un ouvert Ω de $\mathbb{R}^p$ dans $\mathbb{R}^n$ qui est à la fois une immersion dans $\mathbb{R}^n$ et un homéomorphisme de Ω sur un ouvert de M) telle que $g(0) = a$, alors $T_aM = dg(0)\,(\mathbb{R}^p)$.

33.5 Développement

Theorem 33.10. Soit U un ouvert de $\mathbb{R}^n$, $g_1, \dots, g_k : U \mapsto \mathbb{R}$ des fonctions de classe $\mathcal{C}^1$ dont les différentielles sont toutes linéairement indépendantes en chaque point de u. On pose

$$M := \{x \in U \mid g_1(x) = \dots g_k(x) = 0\}$$

Soit $f : U \mapsto \mathbb{R}$ une application différentiable. Si $f_{|M}$ admet un minimum relatif en $x \in M$ alors il existe $\lambda_1, \dots, \lambda_k$ des réels appelés **multiplicateurs de Lagrange** tels que

$$df(x) = \lambda_1 dg_1(x) + \dots + \lambda_k dg_k(x)$$

en d'autre termes, les formes linéaires $df(x), dg_1(x), \dots, dg_k(x)$ sont liées.

Application :

Theorem 33.11 (Théorème Spectral)**.** Soit u un endomorphisme symétrique de $E = \mathbb{R}^n$. Alors E possède une base orthonormée de vecteurs propres de u.

33.6 Preuve

Démonstration.

M est une sous variété de $\mathbb{R}^n$: Posons $g := (g_1, \dots, g_k) : U \mapsto \mathbb{R}^k$. Alors M est défini par l'équation $M = g^{-1}(\{0\})$. Comme les différentielles des g_i sont linéairement indépendantes, g est une submersion. Par le théorème 33.5, M est une sous variété de dimension $n - k$. De plus, l'espace tangeant en x est exactement $T_xM = \ker dg(x) = \bigcap_{i=1}^{k} \ker dg_i(x)$

Si f possède un extremum en x alors la restriction de $df(x)$ à l'espace tangent T_xM est nulle :

Soit $v \in T_xM$ et $\gamma : I \to M$ tel que $\gamma(0) = x$ et $\gamma'(0) = v$. Par construction, la fonction $f \circ \gamma$ possède un extremum relatif en 0 et donc

$$\frac{d}{dt}(f \circ \gamma)(t)_{|0} = 0$$

ie

$$df(\gamma(0)) \cdot \gamma'(0) = df(x) \cdot v = 0$$

.

Donc

$$T_xM \subset \ker df(x)$$

On fait un peu de dualité puisqu'on est en dimension finie

$$\bigcap_{i=1}^{k} \ker dg_i(x) \subset \ker df(x) \iff (\ker df(x))^\perp \subset \left(\bigcap_{i=1}^{k} \ker dg_i(x)\right)^\perp$$
$$\iff Vect(df(x)) \subset \bigoplus_{i=1}^{k} Vect(dg_i(x))$$

Conclusion Par hypothèse, les $dg_i(x)$ forment alors une base de $Vect(dg_i(x))$. Les λ_i sont alors les coordonnées de $df(x)$ dans cette base. □

Application au théorème spectral Soit $u \in S(\mathbb{R}^n)$.

On considère l'application $f : x \mapsto \langle u(x) \mid x\rangle$ et on recherche un maximum sur la sphère $S^{n-1} := \{x \in \mathbb{R}^n \mid g(x) = \|x\|^2 - 1 = 0\}$.

Comme la sphère est compacte (en dimension finie) et que f est continue, on en déduit que f admet bien un maximum en un certain point y.

Par ailleurs, g est bien une application $\mathcal{C}^1$ de differentielle non nulle, car

$$dg(x) \cdot h = 2\langle x \mid h\rangle$$

. En applicant le théorème des extrema liés on en déduit

$$\exists \lambda \in \mathbb{R}, \forall h \in \mathbb{R}^n, \quad df(y) \cdot h = \lambda dg(y) \cdot h = 2\lambda\langle y \mid h\rangle$$

Or,

$$df(y) \cdot h = \langle u(y) \mid h\rangle + \langle u(h) \mid y\rangle = 2\langle u(y) \mid h\rangle$$

par symétrie de u et du produit scalaire. On en déduit donc

$$\forall h \in \mathbb{R}^n, \langle u(y) - \lambda y \mid h\rangle = 0$$

d'où

$$u(y) = \lambda y.$$

Comme y est de norme 1 il n'est pas nul, c'est donc un vecteur propre de u.

On conclut par récurrence en remarquant que $y^\perp$ est stable par u.

CHAPITRE 5

INFO

01 2SAT est NL-Complet + temps linéaire

01.1 Recasages :

— 915 - Classes de complexités. Exemples.

— 916 - Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications.

— 925 - Graphes : Représentations et algorithmes.

01.2 Références :

— [Car14] pour la construction du graphe

— [CLRS02] pour les algos de recherche de CFC.

— [Pap94]

01.3 Comment recaser ce dev ?

— Pour les leçons 915, 916 privilégier la NL complétude. Mais garder en tête qu'on peut le faire en temps linéaire en utilisant un algo de recherche de composantes fortement connexes.

— Pour la leçon 925 c'est clair qu'il faut insister sur l'algo : Kosaraju pour les composantes, évoquer la notion de tri topologique, représentation par matrice d'adjacence pour gagner du temps d'accès.

01.4 Développement

Theorem 01.1. — $2SAT$ est résoluble en temps linéaire.

— $2SAT$ est en fait $NL-$Complet.

L'idée de base de ce développement est la suivante. On a une formule en $2CNF$ et on va voir toute clause de la forme $l_1 \vee l_2$ comme $\neg l_1 \Rightarrow l_2 \wedge \neg l_2 \Rightarrow l_1$ puis on va construire le graphe orienté des implications.

Dans la suite, la taille d'une formule est son nombre de clauses. Puisque la formule est en $2CNF$, il y a au plus deux littéraux par clause, donc linéaire en le nombre de clauses, c'est aussi linéaire en le nombre de littéraux, ou encore en le nombre de variables.

01.5 $2SAT$ en temps linéaire

Etape 0 : On élimine les clauses seules et les clauses triviales Par un simple parcours linéaire de la formule φ, on supprime les clauses triviales, et les doublons ($\psi \wedge C \wedge C \wedge \psi' \equiv \psi \wedge C \wedge \psi'$), et pour chaque clause contenant un unique littéral l on rajoute une variable fraîche x et on remplace cette clause par la clause logiquement équivalente $(l \vee x) \wedge (l \vee \neg x)$. Ceci se fait en un parcours linéraire de la formule. La nouvelle formule obtenue possède au plus le double de clauses.

On supposera donc dans la suite que la formule en entrée possède exactement deux littéraux par clause.

Etape 1 : Construction du graphe

Soit φ une formule en $2CNF$. Soit X l'ensemble des variables apparaissant dans φ. On note $\overline{X}$ l'ensemble des négations de ces variables. On construit un graphe $G_\varphi = (V, E)$ de la façon suivante :

- On pose $V = X \bigsqcup \overline{X}$ l'ensemble des littéraux. On a donc $|V| = O(|\varphi|)$
- Pour chaque clause $l_i \vee l_i'$, $(\neg l_i, l_i') \in E$ et $(l_i, \neg l_i') \in E$. Pour chaque clause on ajoute 2 arêtes, on a donc en particulier $|E| = O(|\varphi|)$.

Remarque Par construction, $l \to l'$ ssi $\neg l' \to \neg l$.

Etape 2 : Caractérisation de la satisfiabilité via le graphe

⚠ **Attention :** Pour la NL-complétude voir ici 01.6. Ne pas trop s'attarder sur l'algo

Lemma .

$$\varphi \text{ est satisfiable } \Leftrightarrow \begin{cases} \forall x \in X, x \text{ et } \neg x \\ \text{ne sont pas dans la même CFC} \end{cases}$$

Démonstration.

$\Rightarrow$ Supposons φ satisfiable et soit ν une valuation positive de φ.

Lemma . Soit l, l' deux sommets tels qu'il existe un chemin $l \rightsquigarrow l'$. Si $\nu(l) = 1$ alors

$\nu(l') = 1$.

Preuve du Lemme. On raisonne par récurrence sur la longueur du chemin. Quitte à considérer le prédécesseur de l' sur le chemin et à appliquer l'hypothèse de récurrence, il suffit de prouver le cas de base $(l, l') \in E$.

Si (l, l') est une arête , alors $\neg l \vee l'$ est une clause de φ donc $\nu(\neg l \vee l') = 1$. Or, $\nu(\neg l) = 0$ par hypothèse. Donc $\nu(l') = 1$. □

Remarque : On en déduit en particulier que toute interprétation satisfaisant φ est constante sur les composantes fortement connexes, et est croissante pour un ordre topologique sur les CFC. Ainsi, s'il existe x tel que x et $\neg x$ sont dans la même CFC la formule n'est pas satisfiable.

$\Leftarrow$ Réciproquement, supposons que pour toute variable x, les littéraux x et $\neg x$ soient dans deux CFC distinctes. On va construire une interprétation $\widetilde{\nu}$ validant φ en raffinant une interprétation partielle. D'après la remarque, $\widetilde{\nu}$ est constante sur les composantes fortement connexes (donc passe au quotient), et est de plus croissante selon un tri topologiqe.

Soit ν une valuation partielle. On note $dom\,\nu$ l'ensemble des littéraux pour lesquels ν est définie. Pendant la construction on va maintenir les invariants suivants :

Ici il faut faire un dessin d'un tri topologique de CFC pour expliquer ce qu'on veut faire

1. $dom\,\nu$ est une union de composantes fortements connexes de G_φ.
2. Si $u \to v$ et $u, v \in dom\,\nu$ alors $\nu(u) \leq \nu(v)$.
3. Si $u \to v$ avec $u \notin dom\,\nu$ et $v \in dom\,\nu$ alors $\nu(v) = 1$.

La construction va procéder en marquant petit à petit les composantes fortement connexes.

1. On utilise l'algorithme de Kosaraju pour obtenir un tri topologique $C_1 \leq \cdots \leq C_k$ des composantes fortement connexes en $O(|E| + |V|) = O(|\varphi|)$. Initialement ces CFC ne sont pas marquées.
2. À l'étape i, on choisit C la composante fortement connexe maximale parmi les CFC non marquées (L'ordre topologique est total).
3. On note $\neg C = \{\neg l \mid l \in C\}$ et on pose $dom\,\nu_{i+1} := dom\,\nu_i \cup C \cup \neg C$.
4. On marque C et C' et
   - Pour tout $v \in C$, on pose $\nu(v) = 1$
   - Pour tout $v \in C'$, on pose $\nu(v) = 0$.

   L'algorithme termine lorsque toutes les composantes fortement connexes ont été marquées et renvoie une interprétation satisfaisant φ.

Preuve de l'algorithme :

- **Terminaison :**
  On vérifie la remarque suivante : Si C est une CFC maximale non marquée alors $\neg C$ est une CFC minimale non marquée :

- $\neg C$ est trivialement une CFC, et est disjointe de C puisque par hypothèse il n'existe aucun littéral l tel que l et $\neg l$ soient dans la même CFC.
- Si $\neg C$ n'est pas minimale parmi les non marquées, il existe une arête $u \to \neg l$ avec $u \notin \neg C$ non marquée et $\neg l \in \neg C$. Mais alors par construction il existe dans le graphe une arête $l \to \neg u$. Or, $l \in C$ et $\neg u$ n'est pas marquée. Ceci contredit la maximalité de C.

En particulier à chaque étape le nombre de CFC non marquées diminue structement et fournit donc un variant assurant la terminaison.

— **Correction :**

- Par construction, ν est définie sur un litéral l ssi ν est définie sur $\neg l$.
- Par la remarque précédente dans la terminaison, ν est constante sur une même CFC, et à chaque étape $dom\,\nu$ est augmenté par l'union (disjointe) de deux CFC. L'invariant 1 est donc bien vérifié et à la fin de l'algorithme toutes les CFC ont été marquées, donc $dom\,\widetilde{nu} = V$ et ν est définie partout.
- Puisque C et $\neg C$ sont toujours disjointe, ν est cohérente au niveau des littéraux et définit bien une valuation de φ.
- Supposons que $u \to v$ avec $u, v \in dom(\nu)$. Si $\nu(v) = 1$ c'est évident. Sinon $\nu(v) = 0$. Donc lorsque la CFC de v a été marquée, elle était minimale parmi toutes les CFC non marquées. Si u est dans cette même CFC, puisque ν est constante sur les CFC on a bien $\nu(u) = \nu(v) = 0$. Sinon, $u \in C' \leq C$. Donc $\neg C' \geq \neg C$ et $\neg C'$ a été choisie avant dans l'algorithme. En particulier, $\nu(\neg C') = 1$ et donc $\nu(C') = 0$. En particulier, $\nu(u) = 0$. L'invariant 2 est donc bien vérifié.
- Si $u \to v$ avec $v \in dom\,\nu$ mais $u \notin dom\,\nu$. Alors u et v ne sont pas dans la même CFC. On note $C(u)$ et $C(v)$ ces deux CFC et on a donc $C(u) \leq C(v)$. Comme $C(u)$ n'est pas marquée, lorsque $C(v)$ a été marquée elle n'était pas minimale parmi les non marquées. Par suite, elle était donc maximale, et s'est vu affecter la valeur 1. Donc $\nu(v) = 1$ et l'invariant 3 est donc vérifié.

Soit à présent $C = l \vee l'$ une clause de φ. Si $\nu(l) = 1$ alors $\nu(C) = 1$. Sinon, $\nu(l) = 0$ et donc $\nu(\neg l) = 1$. Or il existe dans le graphe une arête $\neg l \to l'$. Par croissance, on en déduit que $\neg(l') = 1$ et donc $\nu(C) = 1$. Par conséquent, ν est un modèle de toutes les clauses de φ, donc $\nu \vDash \varphi$.

Complexité : L'algorithme est bien linéaire : Une fois la liste des CFC donnée selon l'ordre topologique, chaque sommet du graphe est visité une fois et une seule pour lui affecter la valuation. □

01.6 NL-Complétude

On propose une variante du point précédent pour prouver plutôt la NL-complétude du problème $2SAT$.

D'après le théorème d'immerman-szelepcsenyi ($\mathbf{NL} = \mathbf{co} - \mathbf{NL}$), il suffit de montrer que $\mathbf{co} - \mathbf{2SAT}$ est $NL - Complet$.

co − 2SAT $\in NL$ Soit φ une formule insatisfiable. On devine de façon non déterministe x tel que x et $\neg x$ sont dans la même CFC et on vérifie que $x \rightsquigarrow \neg x$ et $\neg x \rightsquigarrow x$. Ceci se résume à un problème d'accessibilité dans un graphe. Le graphe n'est jamais stocké puisque les arêtes sont connues directement via les clauses. On utilise donc simplement un espace logarithmique.

co − 2SAT est $NL - hard$ On réduit le problème ACCESS d'accessibilité dans un graphe. Soit (G, s, t) une instance de ACCESS. On va construire φ une formule en 2CNF qui est insatisfiable ssi $s \rightsquigarrow t$ dans G.

Soit $V = \{s, t, v_1, \ldots, v_n\}$ l'ensemble des sommets de G. On va construire φ sur $n+1$ variables $x_0, x_1, \ldots, x_n$. À chaque sommet v_i on associe le littéral positif x_i. À s on associe le littéral positif x_0 et à t on associe le littéral négatif $\neg x_0$. On note μ cette application et on pose alors en mimant la preuve du paragraphe précédent

$$\varphi = \mu(s) \wedge \bigwedge_{(u,v)\in E} \neg\mu(u) \vee \mu(v)$$

— Si $s \rightsquigarrow t$ alors il existe un chemin $s \to u_1 \to \cdots \to u_k \to t$ dans le graphe. Autrement dit, φ possède la formule

$$\mu(s) \bigwedge \left(\neg\mu(s) \vee \mu(u_1) \bigwedge \ldots \bigwedge \neg\mu(u_k) \vee \neg\mu(s)\right)$$

.

Soit ν une valuation de φ.

1. Si $\nu(\mu(s)) = 0$ alors la clause $\mu(s)$ n'est pas satisfaite et $\nu(\varphi) = 0$.
2. Si $\nu(\mu(s)) = 1$ alors par induction sur la longueur du chemin on en déduit que pour que φ soit satisfaite il faut que $\mu(u_i)$ soit évalué à 1 pour tout i. En particulier, la dernière clause $\neg\mu(u_k) \vee \neg\mu(s)$ est évaluée à 0. Absurde.

Donc si t est accessible depuis s, φ est insatisfiable.

Là on fait encore un dessin

— Réciproquement, supposons que $s \not\rightsquigarrow t$. Notons S l'ensemble des sommets accessibles depuis s auquel on rajoute s, T l'ensemble des sommets co-accessibles depuis t augmenté par t. Posons de plus $W := V \backslash (S \cup T)$. Alors S, T, W sont deux à deux disjoints. Soit ν la valuation définie par

$$\nu(\mu(u)) = \begin{cases} 1 & \text{Si } u \in S \sqcup W \\ 0 & \text{Sinon} \end{cases}$$

ν est bien définie puisque $(S \sqcup W) \cap T = \emptyset$ et $\nu \vDash \{\mu(s)\}$. Soit $C := \neg\mu(u) \vee \mu(v)$ une clause de φ. Si $\nu(\mu(u)) = 0$ alors $\nu \vDash C$. Sinon, $\nu(\mu(u)) = 1$ donc $u \in S \sqcup W$. Or, C est une clause de φ donc $(u, v) \in E$. Si $v \in T$ alors $u \to v \rightsquigarrow t$ donc $u \in T$. Absurde. Donc $v \notin T$ et par conséquent $\nu(\mu(v)) = 1$.

Dans tous les cas, $\nu \vDash C$, et par conséquent $\nu \vDash \varphi$. En particulier, φ est satisfiable.

Pour conclure il faut vérifier que la construction peut bien se faire en espace logarithmique. Pour cela, il suffit de ne stocker que des pointeurs vers s et $e \in E$ au lieu de stocker les formules sur la deuxième bande.

02 Ackerman n'est pas récursive primitive

02.1 Recasages :

— 912 - Fonctions récursives primitives et non primitives. Exemples.

02.2 Références :

— [CL03]

02.3 Prérequis :

L'ensemble E des Fonctions récursives primitives est le plus petit ensemble de fonctions de $N^p \to N$ pour $p \geq 0$ tel que :

— E contient toutes les fonctions constantes de $\mathbb{N}^p$ dans $\mathbb{N}$.

— E contient toutes les projections P_p^i pour p et i tels que $1 \leq i \leq p$.

— E contient la fonction successeur.

— E est clos par composition : Si n et p sont des entiers, et si $f_1, \ldots, f_n$ sont des fonctions à p arguments dans E, alors si g est une fonction à n arguments appartenant à E, la fonction $g(f_1, \ldots, f_n)$ à p arguments appartient aussi à E.

— E est clos par récurrence : Si p est un entier, et si $g \in E$ a p arguments, si $h \in E$ a $p+2$ arguments, alors la fonction f définie par récurrence à partir de g et h est aussi dans E :

$$f(x_1, \ldots, x_p, 0) = g(x_1, \ldots, x_p)$$
$$f(x_1, \ldots, x_p, y+1) = h(x_1, \ldots, x_p, y, f(x_1, \ldots, x_p, y))$$

02.4 Développement :

Definition . On définit la fonction d'Ackerman par récurrence :

— $A(0, x) = 2^x$

— $A(n, 0) = 1$

— $A(n+1, x+1) = A(n, A(n+1, x))$

Pour simplifier, on notera aussi $A_n(x) pour A(n, x)$.

Theorem . La fonction A à 2 variables n'est pas récursive primitive.

Remarque : Cette fonction est "intuitivement calculable" mais pourtant, on prouve qu'elle n'est pas récursive primitive. Il manque ainsi des choses pour avoir toutes les fonctions qu'on a envie de calculer.

02.5 Preuve

A_n est gros

Lemma . Pour tout x, $A_n(x) > x$

Démonstration. On va utiliser deux récurrences imbriquées :

Par récurrence sur n : On montre que

$$\forall x, A_n(x) > x$$

:

- Si $n = 0$, $A_0(x) = 2^x > x$.
- Si le résultat est vrai au rang n, prouvons par récurrence sur x que

$$A_{n+1}(x) > x$$

  - Pour $x = 0$, $A_{n+1}(0) = 1 > 0$.
  - Si le résultat est vrai pour x, alors

$$A_{n+1}(x+1) = A_n(A_{n+1}(x))$$

    Or, par hypothèse de récurrence sur n, $A_n(y) > y$ pour tout y. Donc en particulier

$$A_n(A_{n+1}(x)) > A_{n+1}(x)$$

    Puis par l'hypothèse de récurrence sur x,

$$A_{n+1}(x) > x$$

    d'où le résultat.

□

Stricte croissance en x

Lemma . Pour tout entier n, $x \mapsto A_n(x)$ est strictement croissante (en x).

Croissance en n

Lemma . Pour tout entier x, l'application $n \mapsto A_n(x)$ est croissante (en n) pour $n \geq 1$.

Fonctions dominantes :

Definition . Soit $f \in \mathcal{F}_1, g \in \mathcal{F}_p$. On dit que f domine g s'il existe un entier A tel que pour tout $(x_1, x_2, \ldots, x_p)$,

$$g(x_1, \ldots, x_p) \leq f(\sup(x_1, x_2, \ldots, x_p, A))$$

En particulier, si f est strictement croissante, f domine g ssi $g(x_1, \ldots, x_p) \leq f(\sup(x_1, \ldots, x_p))$ sauf pour un nombre fini de $p - uplets$.

Itérées d'ackerman

Definition . On note A_n^k l'itérée $k$eme d'Ackerman : $A_n^0 = Id$ et $A_n^{k+1} = A_n \circ A_n^k$.

Definition . On pose $C_n := \{g \mid \exists k, A_n^k \text{ domine } g\}$ et

$$C := \cup_{n \in \mathbb{N}} C_n$$

Lemma . Pour tout k, n, x,

$$A_n^k(x) \leq A_{n+1}(x + k)$$

Démonstration. Par récurrence sur k :

— Si $k = 0$ alors $A_n^0(x) = x \leq A_{n+1}(x)$.

— Si vrai au rang k alors

$$A_n^{k+1}(x) = A_n(A_n^k(x))$$

Or, par hypothèse de récurrence, $A_n^k(x) \leq A_{n+1}(x + k)$. Par croissance de A_n on en déduit

$$A_n^{k+1}(x) \leq A_n(A_{n+1}(x + k)) = A_{n+1}(x + k + 1)$$

par définition.

□

Theorem . C contient toutes les fonctions récursives primitives.

Démonstration. On prouve le résultat par induction sur les fonctions récursives primitives :

Cas de base : Les fonctions successeur, projecteurs, constantes sont dans C_0.

Composition : Soit $f_1, \dots, f_p, g \in C_n$. Montrons que $Comp(f_1, \dots, f_p, g) \in C_n$.
On dispose de $A_1, \dots, A_p, A$ et $k_1, \dots, k_p, k$ tels que

$$g(y_1, \dots, y_p) \leq A_n^k(\sup(\vec{y}, A))$$

et

$$f_i(x_1, \dots, x_m) \leq A_n^{k_i}(\sup(\vec{x}, A_i))$$

Alors en posant $B = \sup(A_1, \dots, A_p, A)$ et $h := \sup(k_1, \dots, k_p)$,

$$\begin{aligned} g(f_1(x_1, \dots, x_m), \dots, f_p(x_1, \dots, x_m)) &\leq A_n^k(\sup(A_n^{k_1}(\sup(\vec{x}, A_1)), \dots, A_n^{k_p}(\sup(\vec{x}, A_p)), A)) \\ &\leq A_n^k(A_n^h(\sup(\vec{x}, B))) \\ &= A_n^{k+h}(\sup(\vec{x}, B)) \end{aligned}$$

□

Schéma de récurrence : Soit g à p variables, h à $p+2$ variables, et toutes deux dans C_n. Soit A_1, A_2, k_1, k_2 les entiers associés à la domination et $f = Rec(g, h)$. Alors par récurrence sur y :

$$f(x_1, \dots, x_p, y) \leq A_n^{k_1 + yk_2}(\sup(x_1, \dots, x_p, y, A_1, A_2))$$

— Si $y = 0$ alors $f(\vec{x}, 0) = g(\vec{x}) \leq A_n^{k_1}(\sup(\vec{x}, A_1))$ donc le résultat est vrai.

— Supposons la propriété vraie pour y :

$$\begin{aligned} f(\vec{x}, y+1) &= h(\vec{x}, y, f(\vec{x}, y)) \\ &\leq A_n^{k_2}(\sup(\vec{x}, y, f(\vec{x}, y), A_2)) \\ &\leq A_n^{k_2}(\sup(\vec{x}, y, A_n^{k_1+yk_2}(\sup(\vec{x}, y, A_1, A_2)), A_2)) \\ &\leq A_n^{k_2}(A_n^{k_1+yk_2}(\sup(\vec{x}, y, A_1, A_2))) \\ &= A_n^{k_1+(y+1)k_2}(\sup(\vec{x}, y, A_1, A_2)) \\ &\leq A_{n+1}(\sup(\vec{x}, y, A_1, A_2) + k_1 + yk_2) \end{aligned}$$

Cette dernière fonction s'obtient comme composition de fonctions de C_{n+1} donc est encore dans C_{n+1}. Par suite f aussi.

Conclusion : La fonction d'Ackerman n'est dominée par aucune des A_n^k par stricte croissance.

03 Automate d'Aho Corasick

03.1 Recasages :

— 907 - Algorithmique du texte. Exemples et applications.

— 909 - Langages rationnels et Automates finis. Exemples et applications.

03.2 Références :

— [CHL07]

03.3 Prérequis :

Theorem . Soit $X \subset A^\star$ un ensemble fini non vide de mots, ne contenant pas le mot vide. On note $T(X)$ le Trie de X (arbre préfixe) l'automate défini par :

— $Q = Pref(X)$

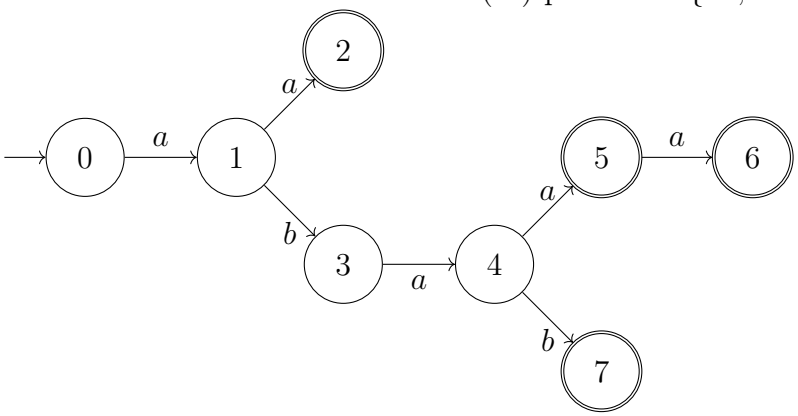
— $I = \{\varepsilon\}$

— $T = X$

— transitions sont (u, a, ua)

Alors, $T(X)$ reconnaît X, et sa construction se fait en temps linéaire en taille de X (notée $|X|$) ie le nombre total de caractères des mots de X. En effet, il suffit de lire des mots et de les enfiler dans la structure lettre par lettre.

FIGURE 5.1 – $T(X)$ pour $X = \{aa, abaaa, abab\}$



03.4 Développement :

L'objectif ici est de reconnaître un motif formé par un ensemble fini de mots. L'utilisation d'un automate est très naturelle : Etant donné un langage fini $X \subset A^\star$, localiser toutes les occurences de mots appartenant à X dans un texte $y \in A^\star$ revient à déterminer tous les préfixes de y qui se terminent par un mot de X ; ce qui revient à reconnaître $A^\star X$, qui est rationnel.

Theorem . Soit $X \subset A^\star$ un ensemble fini non vide de mots, ne contenant pas le mot vide. Alors on peut construire un automate déterministe et complet reconnaissant $A^\star X$.

Plus précisément, soit $h : A^\star \to Pref(X)$ la fonction définie par

$$h(u) = \text{ Le plus long suffixe de } u \text{ qui est un préfixe de } X$$

Alors, l'automate $\mathcal{D}(X)$ défini par

— $Q = Pref(X)$
— $I = \{\varepsilon\}$
— $T = Pref(X) \cap A^*X$
— transitions sont $(u, a, h(ua))$

est déterministe complet et reconnaît $A^\star X$.
Pour calculer h on utilise une autre fonction f définie sur A^+ par

$$f(u) = \text{ Le plus long suffixe propre de } u \text{ qui est un préfixe de } X$$

03.5 Preuve

Dans ce développement, tout d'abord on présente comment on va construire l'automate, en donnant l'intuition de h et f.

Idée :

Comment reconnaître $y \in A^\star X$? On commence par lire y. Tant qu'on reste dans les prefixes de X on peut avancer dans $T(X)$. Si on en sort, c'est qu'on est resté dans la partie $A^\star$. Il faut alors faire du backtrack. Mais il est inutile de revenir trop en arrière, il suffit de récupérer le plus long suffixe qui est un préfixe de X.

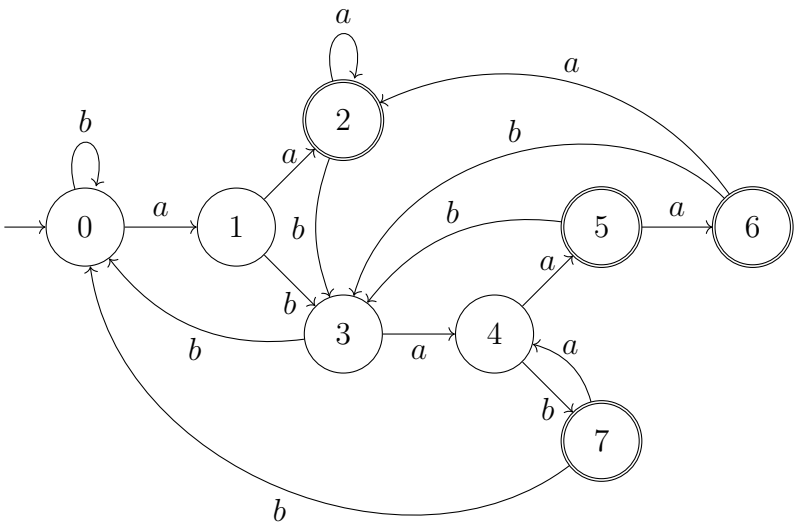
Sauf que la transition après le plus long suffixe qui est un prefixe de X peut être difficile à calculer. En effet, a priori on peut rester sur place et donc ne pas savoir quelle transition appliquer. C'est pourquoi on considère alors le plus long suffixe *Propre*, qui correspond donc à un état strictement antérieur. Il suffit alors de faire un parcours en largeur du Trie pour remplir petit à petit les transitions manquantes !

Intuition : On commence par un lemme trivial mais qu'il faut énoncer.

Lemma .

1. h est croissante pour l'ordre suffixe.
2. Si $x \in Pref(X)$, $h(x) = x$.
3. Pour tout $u \in A^\star$, $h(h(u)) = h(u)$

FIGURE 5.2 – $\mathcal{D}(X)$ pour $X = \{aa, abaaa, abab\}$



Lemma . La fonction h vérifie les propriétés suivantes :

1. $u \in A^\star X$ ssi $h(u) \in A^\star X$ pour tout $u \in A^\star$.
2. $h(\varepsilon) = \varepsilon$
3. $h(ua) = h(h(u)a)$ pour tout $(u, a) \in A^\star \times A$

Démonstration. 1.

$\Rightarrow$ Soit $u \in A^\star X$. Alors $u = vx$ avec $x \in X$. $x \leq u$ donc par croissance, $h(x) \leq h(u)$. Or, $h(x) = x \in X$. Donc $x \leq h(u)$. Par suite, $h(u) = v'x$ où v' est un suffixe de v, ie $h(u) \in A^\star X$.

$\Leftarrow$ Soit $u \in A^\star$ tel que $h(u) \in A^\star X$. Alors $h(u) = vx$ avec $x \in X$. Or, $h(u) \leq u$ et $u = wvx \in A^\star X$.

2. C'est évident.
3. $h(u) \leq u$ donc $h(u)a \leq ua$.
   Par croissance on en déduit
   $$h(h(u)a) \leq h(ua)$$
   D'autre part, $h(ua) \leq ua$. Si $h(ua) = \varepsilon$ alors aucun mot de X ne commence par a. Par suite, $h(h(u)a) = \varepsilon$.
   Sinon, $h(ua) = va$ où $v \leq u$. Comme $h(ua) \in Pref(X)$, on en déduit $v \in Pref(X)$. Par suite, $h(u) \geq v$. Donc
   $$h(ua) = va \leq h(u)a$$
   et par croissance de h,
   $$h(h(ua)) \leq h(h(u)a)$$

Enfin, puisque c'est une involution,

$$h(ua) \leq h(h(u)a)$$

On en déduit le résultat.

□

Theorem . L'automate $\mathcal{D}(X)$ reconnaît $A^\star X$.

Démonstration. — Soit $z \in A^\star$. Par induction sur la longueur du chemin, à l'étape i on est dans l'état $h(z[0 \dots i-1])$. On lit $z[i]$ donc par définition, on arrive dans l'état $h(h(z[0 \dots i-1])z[i])$. Or, par le lemme, ceci est égal à $h(z[0, \dots, i])$.

— Lorsque la lecture de z est finie, on est dans l'état $h(z)$. Il est final, ssi $h(z) \in A^\star X$, ssi $z \in A^\star X$ d'après le lemme.

□

Comment construire $\mathcal{D}(X)$?

Pour construire $\mathcal{D}(X)$, on va introduire une fonction "d'echec" notée f pour "failure function". f est très proche de h, mais n'est définie que sur A^+ :

$$f(u) = \text{ Le plus long suffixe propre de } u \text{ qui est un préfixe de } X$$

L'idée est de procéder à un parcours en largeur de l'arbre préfixe $Trie(X)$, et de compléter les transitions manquantes. Pour cela, on utilise une pile (parcours en largeur), et on empile un couple d'état correspondant à $(u, f(u))$. L'idée est :

Puisque $f(u)$ est *propre*, on aura déjà calculé les transitions issues de $f(u)$ lors du parcours en largeur, et donc on pourra espérer calculer les transitions issues de u.

À l'oral, on admet les lemmes sur f, les preuves sont aussi faciles que pour les lemmes sur h. Il suffit de donner l'intuition, et on prouve la correction de l'algo en donnant l'invariant.

Lemma . Pour tout $(u, a) \in A^\star \times A$ on a

$$h(ua) = \begin{cases} ua & \text{Si } ua \in Pref(X) \\ h(f(u)a) & \text{Si } u \neq \varepsilon \text{ et } u \notin Pref(X) \\ \varepsilon & \text{Sinon} \end{cases}$$

Démonstration. — Si $ua \in Pref(X)$ c'est évident.

— Sinon, si $u = \varepsilon$ c'est aussi évident.

— Sinon, si $h(ua) = \varepsilon$, alors aucun mot de X ne commence par a et $h(f(u)a) = \varepsilon$.

— Sinon, $f(u)a$ est un suffixe de ua dans $Pref(X)$. S'il existe $|v| > 0$ tel que $vf(u)a$ soit un suffixe de ua, appartenant à $Pref(X)$, alors $vf(u)$ est un suffixe de u, dans $Pref(X)$. Par maximalité de $f(u)$, il ne peut-être propre, ie $vf(u) = u$. Mais alors, $vf(u)a = ua \in Pref(X)$, cas qu'on a éliminé. Donc $f(u)a$ est le plus long suffixe de ua, dans $Pref(X)$, ie

$$f(u)a = h(ua)$$

puis

$$h(f(u)a) = h(ua)$$

□

Lemma . Pour tout $(u, a) \in A^\star \times A$ on a

$$f(ua) = \begin{cases} h(f(u)a) & \text{Si } u \neq \varepsilon \\ \varepsilon & \text{Sinon} \end{cases}$$

Démonstration. — Si $u = \varepsilon$, c'est évident.

— Sinon, $u \in A^+$. Alors, si $f(ua) = \varepsilon$, aucun mot de X ne commence par a et donc $h(f(u)a) = \varepsilon$. Sinon, $f(ua) = f(u)a$. Donc $h(f(ua)) = h(f(u)a)$ et puisque $f(ua) \in Pref(X)$, on a $h(f(ua)) = f(ua)$. Par suite

$$f(ua) = h(f(u)a)$$

□

Lemma . Pour tout $u \in A^\star$, $u \in A^\star X$ ssi $x \in X$ ou ($u \neq \varepsilon$ et $f(u) \in A^\star X$).

Faire la preuve

Theorem . L'algorithme du Crochemore [CHL07] est correct et termine.

Algorithm 1 Automate d'Aho-Corasick pour le dictionnaire X

$M \leftarrow Trie(X)$
$q_0 \leftarrow initial[M]$
$F \leftarrow Empty - Queue()$
for a **in** A **do**
  $q \leftarrow Target(q_0, a)$
  if $q = NIL$ **then**
    $Succ[q_0] \leftarrow Succ[q_0] \cup \{(a, q_0)\}$
  else
    $Enqueue(F, (q, q_0))$
  end if
end for
while not $Queue - is - empty(F)$ **do**
  $(p, r) \leftarrow Dequeued(F)$
  if $terminal[r]$ **then**
    $terminal[r] \leftarrow True$
  end if
  for a **in** A **do**
    $q \leftarrow Target(p, a)$
    $s \leftarrow Target(r, a)$
    if $q = NIL$ **then**
      $Succ[p] \leftarrow Succ[p] \cup \{(a, s)\}$
    else
      $Enqueue(F, (q, s))$
    end if
  end for
end while

Démonstration.

Terminaison : Chaque état n'est considéré enfilé qu'au plus une fois à gauche d'un couple.

invariant : La file ne contient que des paires de la forme $(u, f(u))$ et si $f(u)$ est terminal, alors u est terminal :

Cas de base On enfile des couples de la forme (a, ε) où $a \in \Sigma \cap Pref(X)$.

Hérédité : On défile (p, r) qui est donc de la forme $(u, f(u))$. Si $f(u)$ est terminal, alors les lignes 11 et 12 rendent u terminal.

Dans la boucle **for**, on considère des transitions issues de u en lisant a, donc on veut avoir $q = h(ua)$. S'il est déjà défini, c'est que ua est un préfixe de X, et donc $q = ua$. On veut donc enfiler $(ua, f(ua))$. Or, d'après le lemme 03.7, $f(ua) = h(f(u)a)$ ie l'état dans l'Automate $\mathcal{D}(\mathcal{X})$ obtenu en lisant a depuis $f(u)$. C'est ce qui est récupéré dans s ! : $s = h(f(u)a)$. Il suffit donc d'enfiler (q, s).

Sinon, on veut rajouter la transition $(u, a, h(ua))$. D'après le lemme 03.6, $h(ua) = h(f(u)a)$. Or, on a $p = u$ et $r = f(u)$. Puisque c'est un suffixe propre de u, il est distinct

de u, et dans le parcours en largeur on a déjà exploré cet état, et rempli ses transitions. Par conséquent, la transition $(f(u), a, h(f(u)a))$ est déjà présente dans l'automate partiel, et il suffit donc de considérer l'état ciblé en lisant a à partir de $f(u)$. C'est ce qu'on récupère dans s ! Il suffit donc de rajouter la transition (p, a, s). □

04 Algorithme glouton pour SET-COVER

04.1 Recasages :

— 928 - Problèmes NP-Complets : Exemples et réductions.

— 931 - Schémas algorithmiques. Exemples et applications.

04.2 Références :

— [CLRS02]

04.3 Prérequis

Pour parler d'algorithme d'approximation, on a généralement besoin de parler de NP-Complétude dans le cadre de problèmes d'optimisation. Attention à bien définir la NP-complétude dans ce cadre là !

Theorem . Le problème d'optimisation suivant est NP-Complet

ENTRÉE Un couple $(X, \mathcal{F})$ où X est un ensemble fini et $\mathcal{F}$ est un ensemble de sous-ensembles de X, recouvrant icelui :

$$X = \bigcup_{S \in \mathcal{F}} S.$$

SORTIE Un ensemble $\mathcal{C} \subset \mathcal{F}$ minimal tel que

$$X = \bigcup_{S \in \mathcal{C}} S.$$

04.4 Développement

L'algorithme glouton suivant est une approximation de SET-COVER de facteur $O(\log(|X|))$.

Algorithm 2 Algorithme glouton pour SET-COVER

$U \leftarrow X$
$\mathcal{C} \leftarrow \emptyset$
while $U \neq \emptyset$ **do**
  Choisir $S \in \mathcal{F}$ qui maximise $|S \cap U|$.
  $U \leftarrow U - S$
  $\mathcal{C} \leftarrow \mathcal{C} \cup \{S\}$
end while
return $\mathcal{C}$

On note $H(n)$ le *nieme* nombre harmonique. On posera $H(0) = 0$ par commodité.

Theorem . Cet algorithme est un algorithme d'approximation fournissant une garantie de performance $\rho(n)$ à temps polynomial avec

$$\rho(n) := H(\max\{|S| \mid S \in \mathcal{F}\})$$

Démonstration. L'algorithme est clairement polynomial. Pour montrer que c'est un algorithme d'approximation $\rho(n)$ on attribue un coût de 1 à chaque ensemble choisi par l'algorithme, on distribue ce coût sur les éléments couverts pour la première fois puis on uilise ces coûts pour déduire la relation souhaitée entre la taille d'une couverture d'ensemble optimale $\mathcal{C}^*$ et la taille de la couverture d'ensemble $\mathcal{C}$ retournée par l'algorithme. Plus formellement, soit S_i le ieme sous ensemble choisi par l'algorithme glouton. Il génère un coût de 1 quand il ajoute S_i à $\mathcal{C}$. Pour tout $x \in S_i$ non déjà couvert, on attribue alors le coût

$$c_x := \frac{1}{\mid S_i - (S_1 \cup \cdots \cup S_{i-1} \mid}$$

.

Chaque nouvelle étape de l'algorithme assigne un coût unitaire. Donc

$$|C| = \sum_{x \in X} c_x.$$

Le coût de la couverture optimale $C^\star$ est

$$\sum_{S \in C^\star} \sum_{x \in S} c_x$$

$C^\star$ **est une couverture** ie $X = \cup_{S \in C^\star} S$ et donc

$$\sum_{x \in X} c_x \leq \sum_{S \in C^\star} \sum_{x \in S} c_x$$

On en déduit

$$|C| \leq \sum_{S \in C^\star} \sum_{x \in S} c_x$$

On introduit le lemme suivant qu'on démontrera juste après :

Theorem . Pour tout ensemble $S \in \mathcal{F}$,

$$\sum_{x \in S} c_x \leq H(|S|)$$

Finalement :

$$|C| \leq \sum_{S \in C^\star} H(|S|) \leq |C^\star| H(\max |S|)$$

ie

$$\frac{|C|}{|C^\star|} \leq H(\max |S|)$$

D'où le facteur d'approximation.

Preuve du lemme :

Soit un ensemble $S \in \mathcal{F}$. Pour $i = 1, \ldots, |C|$ posons

$$u_i := |S - (S_1 \cup \cdots \cup S_i|$$

le nombre d'éléments de S non encore couverts après l'étape i de l'algorithme. Posons de plus $u_0 = |S|$.

Notons A_i l'ensemble des éléments de S couverts pour la première fois à l'étape i de l'algorithme. Alors $u_{i-1} \geq u_i$ et $u_{i-1} - u_i = |A_i|$.

Soit k l'indice minimal tel que $u_k = 0$ ie la première étape de l'algorithme après laquelle S est entièrement couvert : $S \subset S_1 \cup S_k$.

Alors en partitionnant selon la première étape couvrant chaque élément, $S = \bigsqcup_{i=1}^{k} A_i$ et pour $x \in A_i$,

$$c_x = \frac{1}{|\ S_i - (S_1 \cup \cdots \cup S_{i-1}\ |}$$

Par suite,

$$\begin{aligned}\sum_{x \in S} c_x &= \sum_{i=1}^{k} |A_i| \frac{1}{|\ S_i - (S_1 \cup \cdots \cup S_{i-1}\ |} \\ &= \sum_{i=1}^{k} (u_{i-1} - u_i) \frac{1}{|\ S_i - (S_1 \cup \cdots \cup S_{i-1}\ |}\end{aligned}$$

Or, d'après le choix glouton fait par l'algorithme, S ne peut pas couvrir strictement plus de nouveaux éléments que S_i sinon il aurait été sélectionné à la place de ce dernier. Par conséquent,

$$|S_i - (S_1 \cup \cdots \cup S_{i-1})| \geq |S - (S_1 \cup \cdots \cup S_{i-1})| = u_{i-1}$$

et donc

$$\begin{aligned}\sum_{x \in S} c_x &\leq \sum_{i=1}^{k} (u_{i-1} - u_i) \frac{1}{u_{i-1}} \\ &= \sum_{i=1}^{k} \sum_{j=u_i+1}^{u_{i-1}} \frac{1}{u_i} \\ &\leq \sum_{i=1}^{k} \sum_{j=u_i+1}^{u_{i-1}} \frac{1}{j} \\ &= \sum_{i=1}^{k} \left(\sum_{j=1}^{u_{i-1}} \frac{1}{j} - \sum_{j=1}^{u_i} \frac{1}{j} \right) \\ &= \sum_{i=1}^{k} (H(u_{i-1}) - H(u_i)) \\ &= H(u_0) - H(u_k) \\ &= H(|S|)\end{aligned}$$

□

05 Analyse LL(1) sur un exemple

05.1 Recasages :

— 923 - Analyse lexicale et syntaxique. Applications.

05.2 Références :

— [ASU86]

05.3 Prérequis

Dans la suite, on utilisera le symbole \$ pour terminer une chaîne de caractères.
On rappelle les définitions de FIRSTet FOLLOW.

Definition . Pour tout caractère α, FIRST(α) est l'ensemble des terminaux qui commencent des chaînes dérivées depuis α. Si $\alpha \overset{*}{\Rightarrow} \varepsilon$ alors $\varepsilon \in \text{FIRST}(\alpha)$.

Definition . Pour tout non terminal A on définit FOLLOW(A) comme l'ensemble des terminaux a tels qu'il existe une dérivation de la forme $S \overset{*}{\Rightarrow} \alpha A a \beta$. Si A peut-être le symbole le plus à droite, alors \$ $\in$ FOLLOW(A).

On peut remarque que

1. Si X est terminal, alors $\text{FIRST}(X) = \{X\}$
2. Sinon, si $X \to \varepsilon$ est une règle, alors $\varepsilon \in \text{FIRST}(X)$.
3. Pour toute production $X \to Y_1 Y_2 \dots Y_k$ alors pour tout i tel que

$$\varepsilon \in \text{FIRST}(Y_1) \cap \dots \cap \text{FIRST}(Y_{i-1})$$

et tout $a \in \text{FIRST}(Y_i)$ alors $a \in \text{FIRST}(X)$.

Pour calculer FOLLOWon applique les règles suivantes tant que c'est possible.

1. \$ $\in$ FOLLOW(S) où S est le symbole de départ.
2. Pour toute production $A \to \alpha B \beta$ alors on ajoute $\text{FIRST}(\beta) \backslash \varepsilon$ dans FOLLOW(B).
3. Pour toute production $A \to \alpha B$ ou $A \to \alpha B \beta$ tel que $\varepsilon \in \text{FIRST}(\beta)$ (ie $\beta \overset{*}{\Rightarrow} \varepsilon$) alors on ajoute FOLLOW(A) à FOLLOW(B).

Avec ces deux fonctions FIRSTet FOLLOW, on peut déterminer une table de dérivation à double entrée. Les lignes correspondent à des non terminaux, les colonnes à des symboles d'entrée (terminaux) et la case (i, j) contient l'ensemble des règles applicables à partir du non terminal L_i en lisant le symbole C_j. Lorsqu'aucune règle n'est applicable, la case est vide et le compilateur est censé renvoyer une erreur de syntaxe.

Definition . Une grammaire est dite $LL(1)$ ssi à chaque fois que $A \to \alpha \mid \beta$ sont deux règles de production distinctes,

1. si $\alpha \overset{*}{\Rightarrow} as$ et $\beta \overset{*}{\Rightarrow} bs'$ alors $a \neq b$. (Ils ne dérivent pas de chaînes commençant par la même lettre).
2. Au plus un parmi les deux peut dériver ε.
3. Si $\beta \overset{*}{\Rightarrow} \varepsilon$ alors α ne dérive aucune chaîne commençant par un terminal de FOLLOW(A).

Cela signifie qu'en lisant de gauche à droite (le premier L), on peut réaliser une dérivation gauche (deuxième L) tel qu'il suffit de lire un caractère en avance (fenête de 1) pour choisir la règle. En d'autres termes, chaque case de la table de parsing contient au plus une règle. On peut donc savoir instantanément comment parser une chaîne de caractères !

05.4 Développement

On considère la grammaire G définie par les règles de productions suivantes :

$$E \to TE' \tag{5.1}$$
$$E' \to +TE' \tag{5.2}$$
$$E' \to \varepsilon \tag{5.3}$$
$$T \to FT' \tag{5.4}$$
$$T' \to *FT' \tag{5.5}$$
$$T' \to \varepsilon \tag{5.6}$$
$$F \to (E) \tag{5.7}$$
$$F \to \mathbf{id} \tag{5.8}$$
$$\tag{5.9}$$

où **id** est un lexème identifiant un entier.

Calculons la table d'analyse syntaxique associée à cette grammaire. Pour cela, on commence par calculer les ensembles FIRSTet FOLLOWpour tous les non terminaux.

Je représente ce calcul sous la forme d'un tableau. En colonne je place les non terminaux, et dans les lignes les étapes de calcul. Lorsque plus aucune règle ne s'applique, c'est que j'ai déterminé ces ensembles.

FIRST	E	E'	T	T'	F
1	FIRST(T) (5.1)	$\varepsilon, +$ (5.2, 5.3)	FIRST(F) (5.4)	$\varepsilon, *$ (5.5, 5.6)	$($, **id** (5.7, 5.8)
2	FIRST(T)	$\varepsilon, +$	$($, **id**	$\varepsilon, *$	$($, **id**
3	$($, **id**	$\varepsilon, +$	$($, **id**	$\varepsilon, *$	$($, **id**

FOLLOW	E	E'	T	T'	F
1	\$ (i)				
2	\$,) (5.7)		+ (iii)		∗ (v)
3	\$,)	\$,) (ii)	+		∗
4	\$,)	\$,)	+, \$,) (vi)		∗
5	\$,)	\$,)	+, \$,)	+, \$,) (iv)	∗
6	\$,)	\$,)	+, \$,)	+, \$,)	∗, +, \$,) (vii)

Clarifications :

(i) Le symbole de départ de la grammaire est E donc \$ $\in$ FOLLOW(E).

(ii) Par (5.1), FOLLOW(E) $\subset$ FOLLOW(E')

(iii) Par (5.2), FIRST(E')$\backslash\{\varepsilon\}$ $\subset$ FOLLOW(T)

(iv) Par (5.4), FOLLOW(T) $\subset$ FOLLOW(T')

(v) Par (5.4), FIRST(T')$\backslash\{\varepsilon\}$ $\subset$ FOLLOW(F)

(vi) Puisque $E' \overset{*}{\Rightarrow} \varepsilon$ (5.3) et (5.1) donne $E \to TE'$ on en déduit que FOLLOW(E') $\subset$ FOLLOW(T).

(vii) Puisque $T' \overset{*}{\Rightarrow} \varepsilon$ (5.6) et (5.4) donne $T \to FT'$ on en déduit que FOLLOW(T') $\subset$ FOLLOW(F).

Calcul de la table de Parsing

Pour calculer la table de parsing, on peut remarquer la chose suivante :

— Lorsqu'il existe une production de la forme $A \to \alpha$ et $a \in$ FIRST(α) alors lorsque l'on voit a et que l'on doit dériver A on applique cette règle et on remplace A par α.

— Si $\alpha = \varepsilon$ ou $\alpha \overset{*}{\Rightarrow}$ ça se complique un peu, et on doit remplacer A par α en appliquant cette règle si $a \in$ FOLLOW(A), ou si \$ a été atteint (EOF) et \$ $\in$ FOLLOW(A).

On en déduit la méthode suivante :

1. Pour chaque production $A \to \alpha$ faire les règles (2, 3).
2. Pour chaque terminal $a \in$ FIRST(α), ajouter la règle $A \to \alpha$ dans $M[A, a]$.
3. Si $\varepsilon \in$ FIRST(α), pour chaque terminal $b \in$ FOLLOW(A) on ajoute la règle $A \to \alpha$ dans $M[A, b]$. Si de plus \$ $\in$ FOLLOW(A), on rajoute $A \to \alpha$ dans $M[A, \$]$.

	id	+	∗	(	)	\$
E	$E \to TE'$			$E \to TE'$		
E'		$E' \to +TE'$			$E' \to \varepsilon$	$E' \to \varepsilon$
T	$T \to FT'$			$T \to FT'$		
T'		$T' \to \varepsilon$	$T' \to *FT'$		$T' \to \varepsilon$	$T' \to \varepsilon$
F	$F \to$ **id**			$F \to (E)$		

Exemple d'analyse lexicale + syntaxique On veut parser l'entrée suivante : $5+3*4$

— L'analyseur lexical donne les token suivants : $\langle$**id**, 5$\rangle$, $\langle+\rangle$, $\langle$**id**, 3$\rangle$, $\langle*\rangle$, $\langle$**id**, 4$\rangle$, $\langle\$\rangle$.

— Il ne reste plus qu'à suivre les dérivation gauche en lisant la table qu'on a obtenue. On consomme un token à chaque fois qu'on a une règle $A \to aB$ avec a terminal. Si on ne matche pas l'entrée on renvoie une erreur de syntaxe. Dans le tableau suivant, la tête de pile est à gauche et le fond de pile est symbolisé par \$.

Etape	Règle appliquée	État de la pile	Entrée
0		E\$	$\langle \mathbf{id}, 5\rangle, \langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
1	$E \to TE'$	TE'\$	$\langle \mathbf{id}, 5\rangle, \langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
2	$T \to FT'$	FT'E'\$	$\langle \mathbf{id}, 5\rangle, \langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
3	$F \to \mathbf{id}$	$\mathbf{id}T'E'\$$	$\langle \mathbf{id}, 5\rangle, \langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
4	Consomme Token	$T'E'\$$	$\langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
5	$T' \to \varepsilon$	$E'\$$	$\langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
6	$E' \to +TE'$	$+TE'\$$	$\langle + \rangle, \langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
7	Consomme Token	$TE'\$$	$\langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
8	$T \to FT'$	$FT'E'\$$	$\langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
9	$F \to \mathbf{id}$	$\mathbf{id}T'E'\$$	$\langle \mathbf{id}, 3\rangle, \langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
10	Consomme Token	$T'E'\$$	$\langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
11	$T' \to *FT'$	$*FT'E'\$$	$\langle * \rangle, \langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
12	Consomme Token	$FT'E'\$$	$\langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
13	$F \to \mathbf{id}$	$\mathbf{id}T'E'\$$	$\langle \mathbf{id}, 4\rangle, \langle \$ \rangle$
14	Consomme Token	$T'E'\$$	$\langle \$ \rangle$
15	$T' \to \varepsilon$	$E'\$$	$\langle \$ \rangle$
16	$E' \to \varepsilon$	\$	$\langle \$ \rangle$
17	Fond de pile dans les 2 cas		

06 Correction et complétude du système d'Armstrong

06.1 Recasages :

— 932 - Fondements théoriques de bases de données relationnelles

06.2 Références :

— [Ull82]

06.3 Commentaire

Prendre son temps dans ce développement. Il n'est pas difficile, c'est de la logique, ça va amuser les jury de logique.

> ⚠ **Attention :** Il faut avoir au moins deux éléments distincts dans le domaine des attributs.

06.4 Développement

On considère le système d'inférence d'Armstrong défini par

(FD1) $\dfrac{Y \subset X}{\Gamma \vdash X \to Y}$ (Réflexivité)

(FD2) $\dfrac{\Gamma \vdash X \to Y}{\Gamma \vdash XZ \to YZ}$ (Augmentation)

(FD3) $\dfrac{\Gamma \vdash X \to Y \qquad \Gamma \vdash Y \to Z}{\Gamma \vdash X \to Z}$ (Transitivité)

Augmenté par la règle : $\dfrac{}{\Gamma, \sigma \vdash \sigma}$ (Axiome)

> **Theorem .** Ce système d'inférence est correct et complet : Si F est un ensemble de dépendances fonctionnelles sur un ensemble d'attributs U, et $X \to Y$ une dépendance fonctionnelle sur U. Alors $F \vDash X \to Y$ ssi $F \vdash X \to Y$.

Démonstration.

Correction : Par induction sur l'arbre de dérivation en regardant la dernière règle appliquée.

Complétude :

Etape 1 : On rajoute deux règles

Lemma . Les règles suivantes sont admissibles dans le système d'Armstrong :

— $\dfrac{\Gamma \vdash X \to Y \qquad \Gamma \vdash X \to Z}{\Gamma \vdash X \to YZ}$ (Union)

— $\dfrac{\Gamma \vdash X \to Y \qquad Z \subset Y}{\Gamma \vdash X \to Z}$ (Décomposition)

Preuve du lemme.

— $\dfrac{\dfrac{\Gamma \vdash X \to Y}{\Gamma \vdash X \to XY}(FD2) \qquad \dfrac{\Gamma \vdash X \to Z}{\Gamma \vdash XY \to YZ}(FD2)}{F \vdash X \to YZ}$ (FD3)

— $\dfrac{\dfrac{}{\Gamma \vdash X \to Y} \qquad \dfrac{Z \subset Y}{\Gamma \vdash Y \to Z}(FD1)}{F \vdash X \to Z}$ (FD3)

□

Etape 2 : Cloture relative On définit la cloture de X relativement à F par

$$X_F^+ := \{A \mid F \vdash X \to A\}$$

Lemma . $F \vdash X \to Y$ ssi $Y \subset X_F^+$.

Preuve du lemme.

$\Leftarrow$ Soit $Y = \{A_1, \ldots, A_n\}$ et on suppose que $Y \subset X_F^+$. Alors par définition, $F \vdash X \to A_i$ pour tout i. Par la règle de l'union 06.2, on en déduit que $F \vdash X \to Y$.

$\Rightarrow$ Supposons que $X \to Y$. Alors par la règle de décomposition 06.2 $X \to A_i$ pour tout i, ie $A_i \in X_F^+$. Donc $Y \subset X_F^+$. □

Etape 3 : Preuve de complétude

On raisonne par contraposée en supposant que $F \nvdash X \to Y$. Soit X_F^+ la cloture de X relativement à F et soit $T = \{t_+, t_-\}$ la table à deux tuples définis par $t_+[X_F^+] = t_-[X_F^+]$ mais pour tout $A \notin X_F^+$, $t_+[A] \neq t_-[A]$.

Faire un dessin

T est un modèle de F : Par l'absurde, soit $V \to W \in F$ non satisfaite par T. Alors nécessairement $V \subseteq X_F^+$ et $W \not\subseteq X_F^+$. Soit A un attribut de W qui n'appartient pas à X_F^+. Par définition de la cloture, $F \vdash X \to V$. Donc par (FD3)

$$F \vdash X \to W$$

Comme $A \in W$, alors par (FD1)

$$F \vdash W \to A$$

Donc par (FD3) une nouvelle fois on en déduit

$$F \vdash X \to A$$

et donc $A \in X_F^+$. C'est absurde.

T ne satisfait pas $X \to Y$: Supposons le contraire. Puisque $X \subseteq X_F^+$, t_+ et t_- coïncident sur X. Par la dépendance fonctionnelle, ils coïncident donc sur Y et donc $Y \subseteq X_F^+$. Par suite $F \vdash X \to Y$. Absurde. □

06.5 Postrequis

- À quoi servent les dépendances fonctionnelles ? → Contraintes d'integrité dans une base de données.
- Pour une clef primaire on utilise plutôt un compteur qu'on incrémente.
- Calcul de la cloture relative d'un ensemble d'attributs par saturation. C'est en temps linéaire.
- Problème de la démonstration automatique à cause de la règle de transitivité, qui fait comme une coupure → Pour savoir si $F \vDash X \to Y$ On calcule X_F^+ et on regarde si Y est dedans.
- Faire tourner sur un exemple simple comme $U = \{A_1, A_2, A_3, A_4\}, F = \{A_1 \to A_2A_3, A_2 \to A_3\}, X = \{A_1\}$. Alors $X_F^+ = \{A_1, A_2, A_3\}$.

07 Coût amorti des arbres $2-4$

Faire maaasse dessins dans les preuves

07.1 Recasages :

— 901 - Structures de données. Exemples et applications.
— 921 - Algorithmes de recherche et structures de données associées.
— 926 - Analyse des algorithmes : complexité. Exemples.

07.2 Références :

— Beauquier-Chretienne [BBC92]

07.3 Prérequis :

Les arbres a-b sont des arbres dont toutes les feuilles ont même profondeur, et le nombre de fils d'un noeud varie entre a et b.

Definition . Soient a et b deux entiers, avec $a \geq 2$ et $b \geq 2a-1$. Un arbre $a-b$ est un arbre A vérifiant les conditions suivantes :

— Les feuilles ont toutes la même profondeur
— La racine a au moins 2 et au plus b fils.
— Les autres noeuds ont au moins a et au plus b fils.

On note $d(x)$ le nombre de fils d'un noeud x, et $A_i(x)$ le $i-$eme sous-arbre de x pour $i = 1, \ldots, d(x)$.

— Algorithme de recherche d'une clé $\rightarrow O(\log n)$.
— Insertion d'un élément et rééquilibrage : Règle d'éclatement $\rightarrow O(\log n)$.
— Suppression d'un élément et rééquilibrage : Règles de partage et de fusion $\rightarrow O(\log n)$.

07.4 Développement :

On analyse le coût du rééquilibrage d'un arbre $2-4$ sur une suite d'insertions et de suppressions.

Theorem . On considère une suite quelconque de n insertions ou suppressions dans un arbre $2-4$ initialement vide. Alors le nombre total d'opérations de rééquilibrage est au plus $3n/2$. On a donc un coût amorti constant.

Démonstration.

On commence par donner un exemple rapide de construction ?

La preuve de ce résultat passe par la proposition suivante :

Theorem . On considère une suite quelconque de i insertions et de d suppressions dans un arbre $2-4$ initialement vide, et on pose $n = i + d$. Alors si P désigne le nombre de partages, E le nombre d'éclatements, F le nombre de fusions de sommets on a les inégalités suivantes :

— $P \leq d \leq n$

— $E + F \leq n + (i - d - 1)/2$

Admettons la un instant. Alors

$$E + F + P \leq n + (i - d - 1)/2 + d = n + (i + d - 1)/2 = n + (n - 1)/2 \leq 3n/2$$

La preuve du théorème repose sur une mesure d'équilibre d'un arbre. Un noeud est équilibré si on peut faire une opération d'insertion, ou de suppression sans avoir à le rééquilibrer. Plus précisément :

Definition . Un couple (A, s) est un arbre $2-4$ partiellement équilibré si A est un arbre, s un noeud de A et

— $1 \leq d(s) \leq 5$

— $2 \leq d(x) \leq 4$ pour $x \neq s$.

L'équilibre d'un sommet x partiellement équilibré est le nombre

$$e(x) := \min(d(x) - 2, 4 - d(x)) = \begin{cases} -1 & \text{si } d(x) = 1 \text{ ou } d(x) = 5 \\ 0 & \text{si } d(x) = 2 \text{ ou } d(x) = 4 \\ 1 & \text{si } d(x) = 3 \end{cases}$$

L'équilibre d'un arbre A est la somme des équilibres de ses noeuds :

$$e(A) = \sum_{x \in Noeuds(A)} e(x)$$

Idée : Toute opération d'insertion ou de suppression de feuille dans l'arbre le déséquilibre, alors qu'une opération de fusion, d'éclatement ou de partage le rééquilibre.

On introduit alors une série de lemme qui sont en fait très clairs, on n'en démontre que quelques-uns si on a le temps dans le développement :

Insertion ou suppression déséquilibrent :

Theorem . Soit A un arbre $2-4$, et soit A' l'arbre obtenu après insertion ou suppression d'une feuille, sans rééquilibrage. Alors $e(A') \leq e(A) - 1$.

Theorem . Soit A un arbre $2-4$ à m feuilles. Alors $0 \leq e(A) \leq (m-1)/2$.

Démonstration. On note m_i le nombre de noeuds ayant i fils de sorte que $e(A) = m_3$. Le nombre d'arêtes de l'arbre A est $2m_2 + 3m_3 + 4m_4$. D'autre part, c'est un graphe connexe et acyclique à $m + m_2 + m_3 + m_4$ sommets, donc il possède $m + m_2 + m_3 + m_4 - 1$ arêtes. Par suite,

$$2m_3 = m - 1 - m_2 - 3m_4 \leq m - 1$$

d'où le résulat. □

Eclatement, partage et fusion rééquilibrent :

Theorem Éclatement. Soit (A, s) un arbre $2-4$ partiellement équilibré et supposons que le noeud s a 5 fils. Soit A' l'arbre obtenu par éclatement du noeud s. Alors $e(A') \geq 1 + e(A)$.

Démonstration. A' est un arbre $2-4$ partiellement équilibré. Dans A, $e(s) = -1$. s est sindé en deux sommets s' et s'' d'équilibres 0 et 1.

— Si s est la racine, alors A' a une nouvelle racine r ayant 2 fils s' et s''. Les équilibres des autres sommets ne changent pas. On a alors

$$e(A') = e(A) - e(s) + \underbrace{e(r) + e(s') + e(s'')}_{=1} = e(A) + 2 \geq e(A) + 1$$

— Si s n'est pas la racine, il a un père x, qui sera transformé en un sommet x' à $d(x) + 1$ fils. Les équilibres des autres sommets ne sont pas modifiés donc $e(A') = e(A) - e(x) - e(s) + e(x') + e(s') + e(s'')$ ie

$$e(A') = e(A) - e(x) + 1 + e(x') + 0 + 1 = e(A) + (e(x') - e(x)) + 2$$

. On fait une disjonction de cas selon le nombre de fils de x.

— Si x a 2 fils alors $e(x) = 0$. x' a alors 3 fils, donc $e(x') = 1$ et $e(A') = e(A) + 3$.

— Si x a 3 fils alors $e(x) = 1$. x' a 4 fils donc $e(x') = 0$ et $e(A') = e(A) + 1$.

— Si x a 4 fils alors $e(x) = 0$. x' a 5 fils donc $e(x') = -1$ et $e(A') = e(A) + 1$

□

Theorem Partage. Soit (A, s) un arbre $2-4$ partiellement équilibré dont le sommet s a un seul fils. On suppose que s possède un frère voisin t ayant au moins 3 fils. Soit A' l'arbre obtenu par partage entre s et t. Alors $e(A') \geq e(A)$.

Démonstration. s (d'équilibre -1) est transformé en s' un sommet à 2 fils donc $e(s') = 0$. t est transformé en un sommet t' à $d(t) - 1$ fils. Les autres sommets ne sont pas touchés. Puisque $d(t) \geq 3$ on a bien $d(t') \geq 2$. On obtient donc bien un arbre $2-4$. De plus,

$$e(A') = e(A) - e(s) - e(t) + e(s') + e(t') = e(A) + 1 + (e(t') - e(t))$$

— Si t a exactement 3 fils alors $e(t) = 1$, t' a 2 fils et $e(t') = 0$ donc $e(A') = e(A)$.

— Sinon, t a 4 fils et donc $e(t) = 0$, $e(t') = 1$ et $e(A') = e(A) + 2$.

□

Theorem Fusion. Soit (A, s) un arbre $2-4$ partiellement équilibré dont le sommet s a un seul fils. Soit A' l'arbre obtenu en supprimant s, si s est la racine, et l'arbre obtenu par fusion de s et t si s possède un frère voisin t ayant 2 fils. Alors $e(A') \geq 1 + e(A)$.

Démonstration. — Considérons le cas où s est la racine de A. Si c'est l'unique sommet, alors A' est vide donc $e(A') = 0$ et $e(A) = -1$ d'où $e(A') \geq 1 + e(A)$. Sinon, soit t l'unique sommet de s. Alors A' est l'arbre enraciné en t, et $e(A) = e(A') - e(s) = e(A') - 1$ donc $e(A') \geq e(A) + 1$

— Sinon, s n'est pas la racine. Soit t le frère voisin à 2 fils. $e(t) = 0$. On note t' le noeud de fusion de s et t. Il possède 3 fils, donc $e(t') = 1$. Soit x le père de s et t dans A. x est transformé en x' et $d(x') = d(x) - 1$. On a

$$e(A') = e(A) - e(s) - e(t) - e(x) + e(t') + e(x') = e(A) + 2 + (e(x') - e(x))$$

Par disjonction selon le nombre de fils de x on a $e(x') \geq e(x) - 1$ et donc

$$e(A') \geq e(A) + 1$$

□

À partir des lemmes on peut enfin prouver la proposition

Preuve de 07.3.

Nombre de partages : Il y a au plus un partage par suppression, et aucun par insertion. Donc $P \leq d \leq n$.

Seconde inégalité : Soit A l'arbre obtenu à partir de l'arbre vide apèrs les n opérations d'insertion ou suppression. L'arbre vide a pour équilibre 0. Par ailleurs, chacune des n insertions et suppressions (dans les arbres $2-4$) diminue l'équilibre d'au plus 1 07.5. Chaque éclatement ou fusion l'augmente d'au moins 1 (07.7, 07.9), et chaque partage l'augmente ou le laisse invariant (07.8). Il en résulte que

$$e(A) \geq F + E - n$$

D'autre part, A possède $i - d$ feuilles, donc d'après 07.6

$$e(A) \leq (i - d - 1)/2$$

Finalement

$$E + F \leq n + (i - d - 1)/2$$

□

□

08 NP-complétude de l'équivalence de requêtes conjonctives

08.1 Recasages :

— 928 - Problèmes NP-Complets : Exemples et réductions.

— 932 - Fondements théoriques de bases de données relationnelles

08.2 Références :

— [AHV96] donne la réduction mais ne fait pas la preuve en détail.

08.3 Prérequis :

Il faut être familier avec les requêtes conjonctives sous forme de tableaux, et le théorème d'homomorphisme

> **Theorem .** Soit $q = (T, u)$ et $q' = (T', u')$ deux requêtes tableaux. Alors $q \sqsubseteq q'$ ssi il existe un homomorphisme $\theta : (T', u') \to (T, u)$.

08.4 Développement

> **Theorem .** Le problème suivant est NP-Complet.
>
> **Entrée :** $q = (T, u)$, $q' = (T', u')$ deux requêtes conjonctives.
>
> **Question :** $q' \sqsubseteq q$?

Démonstration. Par le théorème d'homomorphisme $q' \sqsubseteq q$ ssi il existe un homomorphisme $\theta : q \to q'$.

Ce problème est dans NP : Il suffit de deviner une application $\theta : q' \to q$. On peut alors vérifier en temps polynomial que θ est un morphisme.

NP-Hard : On fait une réduction depuis le problème NP-complet Exact-Cover :

> **Entrée :** Un ensemble $X = \{x_1, \ldots, x_n\}$
> et un ensemble $S = \{S_1, \ldots, S_m\}$ tel que $S_i \subseteq X$ pour tout i.
>
> **Question :** Existe-t-il $S' \subseteq S$ tel que S' forme une partition de X ?

Soit (X, S) avec $X = \{x_1, \ldots, x_n\}$ et $S = \{S_1, \ldots, S_m\}$ une instance de exact cover. Soit $A_1, \ldots, A_n, B_1, \ldots, B_m$ des attributs distincts et soit R un schéma de BDD sur ces attributs. Soit $a_1, \ldots, a_n$ des variables distinctes. Posons $u = u' = \langle a_1 : A_1, \ldots, a_n : A_n \rangle$ le sommaire des deux tableaux.

Soit $b_1, \ldots, b_m, c_1, \ldots, c_m$ des nouvelles variables. On construit le tableau T de q de la façon suivante :

— T a n lignes, chaque ligne correspond à un des x_i. On les note $L_{x_1}, \ldots, L_{x_n}$.

— L_{x_i} a a_i pour l'attribut A_i

— L_{x_i} a b_j pour l'attribut B_j pour chaque j tel que $x_i \in S_j$

— L_{x_i} a des nouvelles variables $\widetilde{a_{i,k}}, \widetilde{b_{i,j}}$ pour les autres.

On construit de même le tableau T' de q' :

— T' a m lignes, chaque ligne correspond à un S_i. On les note $L_{S_1}, \ldots, L_{S_m}$.

— L_{S_j} a a_i pour l'attribut A_i pour chaque i tel que $x_i \in S_j$.

— L_{S_j} a c_k pour l'attribut B_k tel que $k \neq j$.

— L_{S_j} a des nouvelles variables $\perp$ pour toutes les autres colonnes.

Exemple :

$X = \{x_1, x_2, x_3, x_4\}$ et $S = \{S_1, S_2, S_3\}$ avec

— $S_1 = \{x_1, x_3\}$

— $S_2 = \{x_2, x_3, x_4\}$

— $S_3 = \{x_2, x_4\}$

Alors on a les tableaux T et T' suivants où les blancs sont des nouvelles variables :

$q :=$

A_1	A_2	A_3	A_4	B_1	B_2	B_3
a_1				b_1		
	a_2				b_2	b_3
		a_3		b_1	b_2	
			a_4		b_2	b_3
a_1	a_2	a_3	a_4			

$q' :=$

A_1	A_2	A_3	A_4	B_1	B_2	B_3
a_1		a_3			c_2	c_3
	a_2	a_3	a_4	c_1		c_3
	a_2		a_4	c_1	c_2	
a_1	a_2	a_3	a_4			

Cette transformation est bien polynomiale.

C'est bien une réduction

> **Theorem .** (X, S) est une instance positive de exact-cover ssi $q' \sqsubseteq q$.

Démonstration.

$\Leftarrow$ On suppose que $q' \sqsubseteq q$. Alors il existe un homomorphisme $\theta : q \to q'$. Il envoie chaque L_{x_i} sur une ligne L_{S_j}. Posons alors S' l'ensemble des S_j correspondant aux lignes de l'image de θ.

— S' **recouvre** X **:** Puisque les sommaires sont égaux, θ induit l'identité sur les a_k. Soit $x_i \in X$. Alors la ligne $L_{S_j} := \theta(L_{x_i})$ possède a_i dans l'attribut A_i ie $x_i \in S_j$.

— S' **est formé d'ensembles disjoints :** Soit $S_i, S_j \in S'$. Supposons qu'il existe $x_{k_0} \in S_i \cap S_j$. Alors

$$L_{x_{k_0}}[B_i] = b_i \text{ et } L_{x_{k_0}}[B_j] = b_j.$$

Soit $L_{x_{i_0}}, L_{x_{j_0}}$ tels que $\theta(L_{x_{i_0}}) = S_i$ et $\theta(L_{x_{j_0}}) = S_j$. Par la remarque précédente, $x_{i_0} \in S_i$ et $x_{j_0} \in S_j$. En particulier, $L_{x_{i_0}}$ possède b_i pour l'attribut B_i. Par suite, $L_{S_i}[B_i] = \theta(b_i)$. D'autre part, par définition, $L_{S_i}[B_i] = \bot$. Donc

$$\theta(b_i) = \bot$$

De même,

$$\theta(b_j) = \bot$$

Soit $L_{S_k} = \theta(L_{x_{k_0}})$. Alors

$$L_{S_k}[B_i] = \theta(b_i) = \bot, \text{ donc } k = i$$

Et de même

$$L_{S_k}[B_j] = \theta(b_j) = \bot, \text{ donc } k = j$$

Finalement,

$$i = j$$

et donc

$$S_i = S_j$$

On a donc prouvé que pour $S_i, S_j \in S'$,

$$S_i \cap S_j \neq \emptyset \Leftrightarrow S_i = S_j$$

S' est donc bien formé d'ensembles disjoints.

Conclusion : On a trouvé un sous-ensemble de S qui forme une partition de X et donc (X, S) est une instance positive de exact cover.

$\Rightarrow$ On suppose que (X, S) est une instance positive de Exact-Cover. Montrons qu'alors $q' \sqsubseteq q$. Soit $S' \subset S$ une partition de X et considérons l'application qui à chaque $x \in X$ associe l'unique S_x de cette partition tel que $x \in S_x$.

$$\theta(a_i) = a_i \text{ pour tout } i. \qquad \theta(b_i) = \begin{cases} \bot & \text{Si } S_i \in S' \\ c_i & \text{Sinon} \end{cases}$$

$$\theta(\widetilde{a_{i,j}}) = \begin{cases} a_j & \text{Si } x_j \in S_{x_i} \\ \bot & \text{Sinon} \end{cases} \qquad \theta(\widetilde{b_{i,j}}) = c_j$$

θ ainsi défini est naturellement prolongeable en une substitution de T. Et $\theta(u) = u = u'$.

Soit $x_i \in X$ et L_{x_i} la ligne de T correspondant à x_i. Montrons que $\theta(L_{x_i}) = L_{S_{x_i}} \in T'$:

$$L_{x_i}[A_j] = \begin{cases} a_i & \text{Si } i = j \\ \widetilde{a_{i,j}} & \text{Sinon} \end{cases}$$

Donc par définition de θ,

$$\theta(L_{x_i})[A_j] = \begin{cases} a_j & \text{Si } x_j \in S_{x_i} \\ \perp & \text{Sinon} \end{cases} = L_{S_i}[A_j]$$

De même,

$$L_{x_i}[B_j] = \begin{cases} b_j & \text{Si } x_i \in S_j \\ \widetilde{b_{i,j}} & \text{Sinon} \end{cases}$$

Donc

$$\theta(L_{x_i})[B_j] = \begin{cases} \perp & \text{Si } S_{x_i} = S_j \\ c_j & \text{Sinon} \end{cases} = L_{S_{x_i}}[B_j]$$

□

Conclusion : On a une réduction polynomiale de exact cover vers le problème d'inclusion de requêtes conjonctives. Ce dernier est donc bien NP-hard. Comme il est dans NP il est donc NP-Complet.

□

09 Calcul de la distance d'édition

09.1 Recasages :

— 907 - Algorithmique du texte. Exemples et applications.

— 931 - Schémas algorithmiques. Exemples et applications.

09.2 Références :

— [CHL07]

09.3 Prérequis

Definition Édition. Soit $u, v \in \Sigma^*$, et $a, b \in \Sigma$. Une édition est de la forme

(i) **Insertion** $uv \to uav$

(ii) **Suppression** $uav \to uv$

(iii) **Modification** $uav \to ubv$

La relation $(\to)$ sur Σ^* définit un système de réécriture.

Theorem . Pour $u, v \in \Sigma^*$ on a toujours $u \to^* v$.

Démonstration. $u \to^* \varepsilon$ en supprimant tous les caractères de u et $\varepsilon \to^* v$ en ajoutant tous les caractères de v. □

Definition Distance d'édition. La distance d'édition $d_E(u, v)$ est la taille de la plus petite dérivation $u \to^* v$.

Theorem . $d_E(u, v) \leq |u| + |v|$

Exemple : Il existe une édition de taille 3 qui mène de rotis à sortie :

$$rotis \to sotis \to sortis \to sortie$$

09.4 Développement

Definition . On appelle *alignement* de u et v la donnée de deux mots de même longueur $\bar{u}, \bar{v} \in \Sigma \sqcup \{\square\}$ tels que si μ est le morphisme effaçant les $\square$, $\mu(\bar{u}) = u$ et $\mu(\bar{v}) = v$.

L'écart d'un alignement est le nombre de lettres qu'il faut modifier entre $\bar{u}$ et $\bar{v}$.

Exemple : Un alignement d'écart 3 entre rotis et sortie

$$\binom{r}{s}\binom{o}{o}\binom{\square}{r}\binom{t}{t}\binom{i}{i}\binom{s}{e}$$

Definition . $d_A(u,v)$ est l'écart du plus petit alignement de u et v.

Theorem . $d_A = d_E$

Démonstration. — Tout alignement peut se traduire en une réécriture de même écart (récurrence sur la longueur de l'alignement). Donc

$$d_A \geq d$$

— Montrons par récurrence sur n que si $u \to^n v$ alors il existe un alignement d'écart $\leq n$: Considérons la dernière réécriture $w \to v$. Que ce soit une insertion, une suppresion ou une modification, on peut traduire en modifiant en conséquence l'alginement et cela n'augmente son écart que d'au plus 1.

□

On en déduit une équation de récurrence :

Theorem . Pour $u, v \in \Sigma^*$, $a, b \in \Sigma$, on a

(i) $d(\varepsilon, u) = |u|$ et $d(u, \varepsilon) = |u|$.

(ii) $d(ua, vb) = min \begin{cases} d(ua,v) & + & 1 \\ d(u,vb) & + & 1 \\ d(u,v) & + & \mathbb{1}_{a=b} \end{cases}$

Démonstration. (i) La relation de réécriture $\to$ ne peut ajouter (ou supprimer) qu'une lettre à la fois.

(ii) On peut faire une réécriture de taille $d(ua,v)+1$ en réécrivant $ua \to^* v$ et en ajoutant b. De même, on peut faire une réécriture de taille $d(u,vb)+1$ et $d(u,v)+\mathbb{1}_{a=b}$. Par suite,

$$d(ua, vb) \leq min \begin{cases} d(ua,v) & + & 1 \\ d(u,vb) & + & 1 \\ d(u,v) & + & \mathbb{1}_{a=b} \end{cases}$$

Montrons qu'on a en fait l'égalité : Considérons un alignement optimal entre ua et vb et faisons une disjonction de cas selon la dernière règle utilisée :

— Supposons que la dernière paire est une modification (potentiellement de coût nul) $\binom{a}{b}$. Alors le reste est nécessairement un alignement optimal pour u et v (sinon on pourrait faire mieux ce qui contredirait l'optimalité pour ua, vb). L'écart de cet alignement est donc $d(u,v)+\mathbb{1}_{a=b}$.

— Si la dernière paire est une insertion $\binom{\square}{b}$ alors le reste est un alignement optimal pour ua, v. L'écart de cet alignement est donc $d(ua,v)+1$

— Si la dernière paire est une suppression $\binom{a}{\square}$ alors le reste est un alignement optimal pour u, vb. L'écart de cet alignement est donc $d(u, vb) + 1$.

□

On en déduit l'algorithme suivant qui exploite la programmation dynamique : On a des sous problèmes (les sous-alignements), et on en déduit la longueur d'un alignement optimal entre u et v.

La case $T[i, j]$ est la distance d'édition entre un prefixe de taille i de u et un prefixe de taille j de v. On initialise tout d'abord avec la distance d'un prefixe de taille i (resp. j) à ε. Puis on utilise l'équation de récurrence.

Algorithm 3 Calcul de la distance d'édition entre u, v

$T \leftarrow Tableau(|u| + 1, |v| + 1)$

 # Initialisation : $d(u[1, \ldots, i], \varepsilon) = i$
for $0 \leq i \leq |u|$ **do**
  $T[i, 0] \leftarrow i$
end for

 # Initialisation : $d(\varepsilon, v[1, \ldots, j]) = j$
for $0 \leq j \leq |v|$ **do**
  $T[0, j] \leftarrow j$
end for

for $1 \leq i \leq |u|$ **do**
  for $1 \leq j \leq |v|$ **do**
    if $u[i] = v[j]$ **then**
      $T[i, j] \leftarrow \min(T[i-1, j] + 1, T[i, j-1] + 1, T[i-1, j-1])$
    else
      $T[i, j] \leftarrow \min(T[i-1, j] + 1, T[i, j-1] + 1, T[i-1, j-1] + 1)$
    end if
  end for
end for

10 Problèmes indécidables et grammaires algébriques

10.1 Recasages :

— 914 - Décidabilité et indécidabilité. Exemples.

— 923 - Analyse lexicale et syntaxique. Applications.

10.2 Références :

— [Car14]

10.3 Comment recaser ce dev ?

— Il est évidemment clair dans la 914.

— Pour la leçon 923 insister dans le plan sur le fait qu'il faille des grammaires non ambiguës pour parser efficacement. Et paf, c'est en fait indécidable. Mais on peut aller plus loin dans l'indécidabilité, puisque même savoir si une grammaire engendre un rationnel est indécidable. Ça rejoint le rapport de Jury sur les différences entre langages algébriques et langages rationnels. On comprend donc pourquoi pour l'analyse syntaxique il faut des outils plus puissants que pour la simple analyse lexicale.

10.4 Développement :

Theorem Vide de l'Intersection. Le problème suivant est indécidable

DONNÉE G_1, G_2 gramaires algébriques

QUESTION $\mathcal{L}(G_1) \cap \mathcal{L}(G_2) = \emptyset$

Démonstration. On effectue une réduction depuis le problème de correspondance de Post :

Theorem PCP. Le problème suivant est indécidable :

DONNÉE Un entier $m \geq 1$ et une suite $(u_1, v_1), \ldots, (u_m, v_m)$ de paires de mots sur un alphabet Σ.

QUESTION Un entier $n \geq 1$ et une suite d'indices $i_1, \ldots, i_n$ de $\{1, \ldots, m\}$ telle que

$$u_{i_1} u_{i_2} \cdots u_{i_n} = v_{i_1} v_{i_2} \cdots v_{i_n}$$

Soit donc $(u_i), (v_i)$ une instance de PCP. Pour tout $i \in \{1, \ldots, n\}$ on associe un caractère frais x_i de sorte que les x_i soient tous distincts. Soit $\#$ un autre nouveau caractère. On pose $\Sigma' := \Sigma \sqcup \{\#\} \sqcup \{x_1, \ldots, x_n\}$

On définit alors sur cet alphabet deux grammaires :

$$G_1 : S_1 \to u_i S_1 x_i \mid u_i \# x_i$$

et

$$G_2 : S_2 \to v_i S_2 x_i \mid v_i \# x_i$$

Si l'intersection est non vide, il y a une solution à PCP

Supposons que les langages de ces deux grammaires aient un mot w en commun. Alors

$$\begin{aligned} w &= u_{i_1} \dots u_{i_k} \# x_{i_k} \dots x_{i_1} \\ &= v_{j_1} \dots v_{j_l} \# x_{j_l} \dots x_{j_1} \end{aligned}$$

(par induction sur la dérivation).

Puisque les x_i sont tous distincts, on en déduit que $k = l$ et $i_1 = j_1, \dots, i_k = j_l$. Par suite, on a l'égalité

$$u_{i_1} \dots u_{i_k} = v_{i_1} \dots v_{i_k}$$

Enfin, $k \geq 1$ car $\# \notin \mathcal{L}(G_i)$.

S'il y a une solution à PCP, l'intersection est non vide

Réciproquement, supposons que l'on dispose d'une solution $(n \geq 1, i_1, \dots, i_n)$ de PCP. Alors le mot

$$\begin{aligned} w &= u_{i_1} \dots u_{i_n} \# x_{i_n} \dots x_{i_1} \\ &= v_{i_1} \dots v_{i_n} \# x_{i_n} \dots x_{i_1} \end{aligned}$$

est dans l'intersection de ces deux langages. □

Theorem Ambiguïté. Le problème suivant est indécidable

DONNÉE G une grammaire.

QUESTION G est ambiguë ?

Démonstration. Remarquons que dans la réduction précédente, les deux grammaires G_1, G_2 sont non ambiguës. On a donc prouvé le théorème suivant :

Theorem . Le problème suivant est indécidable

DONNÉE G_1, G_2 deux grammaires non ambiguës.

QUESTION $\mathcal{L}(G_1) \cap \mathcal{L}(G_2) = \emptyset$?

Réduisons ce problème de l'intersection de deux grammaires non ambiguës. Soit G_1, G_2 deux grammaires non ambiguës, de symboles de départ S_1, S_2. On construit alors la grammaire G de symbole initial S, dont les règles de productions sont l'union des règles de G_1 et G_2, à laquelle on a rajouté la règle $S \to S_1 \mid S_2$.

Puisque G_1 et G_2 sont non ambiguës, un mot de $\mathcal{L}(G)$ possède deux dérivations ssi il peut être dérivé à la fois par G_1 et par G_2. Autrement dit, G est ambiguë ssi $\mathcal{L}(G_1) \cap \mathcal{L}(G_2) \neq \emptyset$. □

On admet le théorème suivant

Theorem Universalité. Le problème suivant est indécidable :
DONNÉE G une grammaire algébrique.
QUESTION $\mathcal{L}(G) = \Sigma^*$?

Et on prouve

Theorem Rationnalité. Le problème suivant est indécidable :
DONNÉE G une grammaire algébrique.
QUESTION $\mathcal{L}(G)$ est rationnel ?

Démonstration. Soit G une grammaire algébrique sur un alphabet Σ. Considérons L_2 un langage algébrique mais non rationnel sur un alphabet disjoint Γ. Posons

$$L = \Sigma^* \# L_2 \cup \mathcal{L}(G) \# \Gamma^*$$

où $\#$ est un symbole frais.

L est algébrique et on peut calculer sa grammaire en fonction de G et de la grammaire de L_2. Montrons que L est rationnel ssi $\mathcal{L}(G) = \Sigma^*$:

Supposons L rationnel et par l'absurde $\mathcal{L}(G) \neq \Sigma^*$. Soit $y \in \Sigma^* \backslash \mathcal{L}(G)$. Comme L est rationnel, le langage suivant est encore rationnel :

$$L \cap y\#\Gamma^*$$

Or,

$$L \cap y\#\Gamma^* = y\#L_2$$

On en déduit par stabilité par quotient à gauche que le langage $(y\#)^{-1}y\#L_2 = L_2$ est rationnel. Absurde.

Réciproquement, supposons $\mathcal{L}(G) = \Sigma^*$. Alors $L = \Sigma^*\#\Gamma^*$ est bien rationnel. □

10.5 Postrequis

On peut adapter la preuve pour avoir un analogue du théorème de rice dans le cadre des grammaires algébriques :

Toute propriété non triviale sur les langages algébriques, qui est vraie sur les rationnels, stable par intersection avec un rationnel, et stable par quotient par un rationnel est indécidable.

11 Hachage Parfait

11.1 Recasages :

— 901 - Structures de données. Exemples et applications.

— 921 - Algorithmes de recherche et structures de données associées.

— 926 - Analyse des algorithmes : Complexité. Exemples.

11.2 Références :

— [CLRS02]

11.3 Prérequis :

— Notion de table de hachage.

— Résolution des collisions par chaînage.

Definition Famille universelle de fonctions de hachage. Une collection finie $\mathcal{H}$ de fonctions de hachage qui créent une correspondance entre un univers $\mathcal{U}$ de clefs et $\{0, \dots, m-1\}$ est *Universel* si pour chaque paire de clefs $k \neq l \in \mathcal{U}$ le nombre de fonctions de hachage pour lesquelles $h(k) = h(l)$ est $\leq \mathcal{H}/m$ ie en mettant la probabilité uniforme sur $\mathcal{H}$:

$$\forall k, l \in \mathcal{U}, k \neq l \Rightarrow \mathbb{P}(h(k) = h(l)) \leq \frac{1}{m}$$

Definition . — Soit p premier grand tel que toute clef k soit dans l'intervalle $\{0, \dots, p-1\}$.

— Soit m le nombre d'alvéoles de la table de hachage.

Pour $(a, b) \in \mathbb{Z}/p\mathbb{Z}^\star \times \mathbb{Z}/p\mathbb{Z}$ on pose

$$h_{a,b} : \left\{ \begin{array}{rcl} \mathbb{Z}/p\mathbb{Z} & \to & \mathbb{Z}/m\mathbb{Z} \\ k & \mapsto & ((ak+b) \mod p) \mod m \end{array} \right.$$

et $\mathcal{H}_{p,m} := \{h_{a,b} \mid (a, b) \in \mathbb{Z}/p\mathbb{Z}^\star \times \mathbb{Z}/p\mathbb{Z}\}$.

Theorem . $\mathcal{H}_{p,m}$ est une famille universelle de fonctions de hachage.

11.4 Développement :

Theorem . Si l'espace des clefs est *statique* (ie connu à l'avance), on peut trouver une méthode de hachage telle que *dans le pire cas* la recherche soit en temps $O(1)$, en utilisant seulement un espace linéaire.

Idée :

Dans le hachage, ce qui prend du temps c'est la résolution des collisions. La première idée est de trouver des fonctions de hachage qui n'en ont pas. Mais ceci peut prendre du temps. Fort heureusement, les familles universelles de fonctions de hachage existent

Theorem . Si on stocke n clefs dans une table de hachage de taille m via une fonction de hachage $h \sim \mathcal{U}(\mathcal{H})$ où $\mathcal{H}$ est une famille universelle, alors l'espérance du nombre de collisions est inférieur à

$$\binom{n}{2}\frac{1}{m}$$

Démonstration. Soit X la variable aléatoire dénombrant les collisions. Pour $k \neq l$ posons $X_{k,l} := \mathbb{1}_{h(k)=h(l)}$. Alors

$$X = \sum_{k \neq l} X_{k,l}$$

donc par linéarité

$$\begin{aligned}\mathbb{E}(X) &= \sum_{k \neq l} \underbrace{\mathbb{P}(h(k) = h(l))}_{\leq 1/m} \\ &\leq \frac{1}{m} \sum_{k \neq l} 1 \\ &= \frac{1}{m}\binom{n}{2}\end{aligned}$$

□

Espace quadratique :

Faire un dessin

Si on s'autorise un espace quadratique, alors une fonction de hachage universelle n'a pas trop de collisions :

Theorem . Si on stocke n clefs dans une table de hachage de taille $m = n^2$ via une fonction de hachage tirée uniformément dans une famille universelle, alors la probabilité d'avoir des collisions est $< 1/2$. Plus précisément, si X dénombre les

collisions, alors

$$\mathbb{P}(X \geq 1) < \frac{1}{2}.$$

Démonstration. D'après le lemme précédent, $\mathbb{E}(X) \leq \frac{1}{n^2}\binom{n}{2} = \frac{1}{2} - \frac{1}{2n} < \frac{1}{2}$ Alors par l'inégalité de Markov,

$$\mathbb{P}(X \geq 1) \leq \frac{\mathbb{E}(X)}{1} < \frac{1}{2}$$

□

On peut alors tirer h aléatoirement et recommencer tant qu'il y a des collisions.

Le nombre de tirages à faire suit une loi géométrique de paramètre $1-\mathbb{P}(X \geq 1) > 1/2$ donc l'espérance du nombre de tirages à faire est $\frac{1}{1-\mathbb{P}(X \geq 1)} < 1/2$, et la variance est $\frac{\mathbb{P}(X \geq 1)}{(1-\mathbb{P}(X \geq 1))^2} < 1/8$.

On dispose donc ici d'une méthode de hachage nécessitant un espace quadratique. Peut-on faire mieux ?

Espace linéaire :

On va essayer de se limiter à seulement n cases. On aura donc nécessairement des collisions. L'idée est d'utiliser des tables de hachages secondaires pour résoudre ces collisions, et de faire un hachage parfait sur chacune d'entre elle.

Faire un Dessin !!

L'alvéole j contient à présent un pointeur vers une table de hachage T_j de taille m_j et contenant n_j éléments. Alors $n = \sum_{j=1}^{k} n_j$. On va utiliser du hachage parfait, de sorte que $m_j = n_j^2$.

Plus formellement, notons $n_0, \ldots, n_{n-1}$ le nombre de clefs hachées vers les cases $0, \ldots, n-1$. On réalise un hachage parfait pour chaque alvéole.

Theorem . Si on stocke n clés dans une table de hachage de taille n via une fonction h tirée uniformément sur $\mathcal{H}_{p,n}$ alors

$$\mathbb{E}(|T_0| + \cdots + |T_{n-1}|) = \mathbb{E}(\sum_{j=0}^{n-1} n_j^2) < 2n$$

Démonstration. On remarque que $a^2 = a + 2\binom{a}{2}$. Alors

$$\begin{aligned}\mathbb{E}\left(\sum_{j=1}^{n} n_j^2\right) &= \mathbb{E}\left(\sum_{j=1}^{n} n_j + 2\binom{n_j}{2}\right)\\ &= \mathbb{E}\left(\underbrace{\sum_{j=1}^{n} n_j}_{=n}\right) + 2\,\mathbb{E}\left(\sum_{j=1}^{n}\binom{n_j}{2}\right)\\ &= n + 2\,\mathbb{E}\left(\sum_{j=1}^{n}\binom{n_j}{2}\right)\end{aligned}$$

Or, $\binom{n_j}{2}$ est le nomre de paires d'éléments distincts dans T_j. Donc $\sum \binom{n_j}{2}$ est le nombre total de paires qui ont collisionné sous h. D'après le lemme 11.5,

$$\mathbb{E}\left(\sum_{j=1}^{n}\binom{n_j}{2}\right) \leq \frac{1}{n}\binom{n}{2} = \frac{n-1}{2}$$

Par suite,

$$\mathbb{E}\left(\sum_{j=1}^{n} n_j^2\right) \leq 2n - 1 < 2n$$

□

On en déduit finalement le corollaire suivant :

Theorem . Si l'on stocke n clés dans une table de hachage de taile $m = n$ via une fonction de hachage h choisie uniformément dans une classe universelle de fonctions de hachage, et si l'on prend pour chaque table de hachage secondaire une taille $m_j = n_j^2$ alors la probabilité que l'espace total consommé pour les tables de hachage secondaires dépasse $4n$ est inférieure à $1/2$

Démonstration. On applique l'inégalité de Markov :

$$\begin{aligned}\mathbb{P}(|T_0| + \cdots + |T_{n-1}| \geq 4n) &\leq \frac{\mathbb{E}(|T_0| + \cdots + |T_{n-1}|)}{4n}\\ &< \frac{1}{2}\end{aligned}$$

□

Il suffit alors de tester un petit nombre de fonctions de hachage secondaires dans un prétraitement pour obtenir un hachage parfait en espace linéaire.

Ces tests ses font via des tours de boucles, et ensuite la recherche d'un élément est $O(1)$.

11.5 Postrequis

Postrequis Hachage parfait

—

12 Théorème de hierarchie en espace et en temps

12.1 Recasages :

— 913 - Machines de TURING. Applications.

— 915 - Théorème de hierarchie en espace et en temps.

12.2 Références :

— [Per14]

12.3 Prérequis :

Theorem Machine universelle. Il existe une machine de Turing U à 5 bandes, sur l'alphabet d'entrée $\sigma_U = \{0,1\}$ et l'alphabet de travail $\Gamma_U = \{0,1,B\}$, telle que pour toute machine M sur les alphabets Σ_M, Γ_M :

— Il existe un morphisme $\varphi_M : \Sigma_M^\star \to \Sigma_U^\star$ tel que pour tout mot $x \in \Sigma_M^\star$, le calcul de la machine U sur le couple $(\langle M\rangle, \varphi_M(x))$ simule $M(x)$.

— Il existe une constante α_M telle que pour tout $x \in \Sigma_M^\star$, si $M(x)$ s'arrête en temps t et utilise un espace s alors $U(\langle M\rangle, \varphi_M(x))$ s'arrête en temps $\leq \alpha_M(1+t^2)$ et en espace $\leq \alpha_M(1+s)$.

Definition . Une fonction $t : \mathbb{N} \to \mathbb{N}$ est *constructible en temps* s'il existe une constante α et une machine de Turing M qui sur l'entrée 1^n (n en unaire) renvoie $1^{t(n)}$ ($t(n)$ en unaire) en temps $\leq \alpha t(n)$.

Definition . Une fonction $s : \mathbb{N} \to \mathbb{N}$ est *constructible en espace* s'il existe une constante α et une machine de Turing M qui sur l'entrée 1^n (n en unaire) renvoie $1^{s(n)}$ ($s(n)$ en unaire) en utilisant un espace $\leq \alpha s(n)$.

La plupart des fonctions usuelles de complexité sont constructibles en temps et en espace. Par exemple :

— $t(n) = c$ pour une constante $c \in \mathbb{N}$ est constructible en temps et en espace.

— $s(n) = \lfloor \log(n) \rfloor$ est constructible en espace.

— $t(n) = s(n) = n$ est constructible en espace et en temps.

— $t(n) = s(n) = 2^n$ est constructible en espace et en temps.

— Si s et s' sont constructibles en espace alors il en est de même de leur produit et de leur somme. Ainsi tous les $\lfloor \log(n) \rfloor^k$ et les polynômes sont constructibles en espace.

— Si t et t' sont constructibles en temps alors il en est de même de leur produit et de leur somme. Ainsi tous les polynômes sont constructibles en espace.

Remarque : Si une fonction $f(n)$ est constructible en temps et vérifie $f(n) = o(n)$ alors f est ultimement constante. Pour voir ça, remarquer qu'une machine fonctionnant en temps $o(n)$ se comporte de la même façon sur les entrée 1^n et 1^{n+1} pour n suffisamment grand.

Exemple de preuve de constructibilité : Montrons que $\lfloor \log(n) \rfloor$ est constructible en espace.

Pour cela, on considère la machine M suivante :

— Sur l'entrée x, la machine M commence par vérifier que x est de la forme 1^n en se déplaçant sur la bande de lecture. N'utilise pas d'espace supplémentaire.

— Si $x = 1^n$, la machine initialise un compteur binaire à 0 sur la bande de travail. Par commodité, le compteur aura son bit de poids faible à gauche.

— On parcourt l'entrée de gauche à droite tant que le symbole 1 est lu.

— À chaque étape, le compteur est incrémenté de 1. Ceci ne nécessite pas d'espace supplémentaire (analogue à un automate fini, la machine se positionne sur le bit de poids faible. Tant qu'elle lit 1, elle réécrit 0 à la place (propagation de la retenue). Si elle lit 0, elle le remplace par un 1 et ramène la tête de lecture à gauche. Si elle lit un B, elle le remplace par 1 et ramène la tête à gauche).

— Enfin on parcourt la valeur finale du compteur à partir de la deuxième case, et dès qu'on lit 0 ou 1 on écrit 1 sur la bande de sortie.

À la fin, le compteur représente l'entier n en binaire, donc est écrit sur $1 + \lfloor \log(n) \rfloor$ bits. En lisant à partir de la deuxième case, on écrit bien $\lfloor \log(n) \rfloor$ en unaire.

12.4 Développement :

Theorem Hierarchie en temps. Soit $f : \mathbb{N} \to \mathbb{N}$ et $g : \mathbb{N} \to \mathbb{N}$ des fonctions telles que g soit constructible en temps et $f^2 = o(g)$. Alors

$$DTIME(f(n)) \subsetneq DTIME(g(n))$$

Theorem Hierarchie en espace. Soit $f : \mathbb{N} \to \mathbb{N}$ et $g : \mathbb{N} \to \mathbb{N}$ des fonctions telles que g soit constructible en espace et $f = o(g)$. Alors

$$DSPACE(f(n)) \subsetneq DSPACE(g(n))$$

12.5 Preuve :

Hierarchie en temps.

Idée :

Il s'agit de construire un langage $L \in DTIME(g(n))$ tel que $L \notin DTIME(f(n))$. Pour cela, on va construire une machine V fonctionnant en temps $g(n)$ mais telle que toute machine M fonctionnant en temps $f(n)$ se trompe sur au moins une entrée de $\mathcal{L}(V)$. L'idée est encore de diagonaliser en considérant un langage de la forme $\{\langle M\rangle \mid M(\langle M\rangle)$ rejette en temps $\leq f(n)$ Avec $n = |\langle M\rangle|\}$. Mais le coût de la simulation dépend de M donc il est difficile de le gérer. Pour cela, on va légèrement modifier l'entrée :

Modification de l'entrée :

On commence par augmenter l'entrée du problème en considérant les entrées de la forme $(\langle M\rangle, x)$ où x est un mot arbitraire.

Construction de la machine

Soit U la machine de Turing universelle du théorème 12.1 et considérons la machine V suivante :

Algorithm 4 Machine de Turing V sur l'entrée $(\langle M\rangle, x)$

Calcule $g(n)$ où $n = |(\langle M\rangle, x)|$.
Exécute $U(\langle M\rangle, (\langle M\rangle, x))$ pendant $g(n)$ étapes en avançant à chaque étape dans la lecture de $g(n)$.
if U n'a pas terminé le calcul **then**
  REJETER
else
  if U a terminé en acceptant **then**
    REJETER
  else
    ACCEPTER
  end if
end if

On note L le langage reconnu par V. V est déterministe.

1. V calcule tout d'abord $g(n)$ pour savoir quand s'arrêter. Puisque g est constructible en temps, ceci prend un temps $O(g(n))$.
2. Ensuite, V simule $g(n)$ étapes du calcul de M sur l'entrée $(\langle M\rangle, x)$.

On en déduit que V calcule en temps $O(g(n))$, et donc $L \in DTIME(g(n))$.

L $\notin$ DTIME$(f(n))$

En effet, soit M une machine fonctionnant en temps $\leq Cf$. Alors U simule M en temps $\leq \alpha_M C f^2$. Or, $f^2(n) = o(g(n))$ donc pour n assez grand,

$$g(n) \geq \alpha_M C^2 f(n)^2$$

et donc pour x assez grand (c'est là qu'on utilise x !!), la simulation de M sur $(\langle M\rangle, x)$ par U termine en temps $\leq g(n)$. Alors :

— Si M accepte $(\langle M\rangle, x)$ alors $V(\langle M\rangle, x)$ rejette et $(\langle M\rangle, x) \notin L$.

— Si M rejette $(\langle M\rangle, x)$ alors $V(\langle M\rangle, x)$ accepte et $(\langle M\rangle, x) \in L$.

Ainsi, si M reconnaît L on a d'une part $M(\langle M\rangle, x) = V(\langle M\rangle, x)$ et d'autre part $V(\langle M\rangle, x) = \neg M(\langle M\rangle, x)$ puisque la simulation termine. Donc $M(\langle M\rangle, x) = \neg M(\langle M\rangle, x)$. Absurde. □

Hierarchie en Espace.

Idée : L'idée est essentiellement la même, en utilisant cette fois-ci l'espace. On construit une machine V' qui sur l'entrée $(\langle M\rangle, x)$:

1. Commence par calculer $g(n)$ en unaire (prend un espace $O(g(n))$ puisque g est constructible en espace).
2. Simule M sur $(\langle M\rangle, x)$, en décalant la tête de lecture sur le compteur dans le même sens pour vérifier qu'on ne dépasse pas l'espace $g(n)$.
3. Si on dépasse, on rejette.
4. Si on termine la simulation, on renvoit l'opposé.

Le reste de la preuve est identique.

□

13 Sémantique axiomatique de l'exponentiation rapide

13.1 Recasages :

— 927 - Exemples de preuve d'algorithmes : Correction, terminaison.

— 930 - Sémantique des langages de programmation. Exemples.

13.2 Références :

— [Win93] traite le cas de la factorielle.

13.3 Prérequis

On rappelle les règles de la logique de Hoare :

$$\textbf{skip :} \quad \frac{}{\{P\}\ \textbf{skip}\ \{P\}}$$

$$\textbf{Affectation :} \quad \frac{}{\{P[x \mapsto e]\}\ x := e\ \{P\}}$$

$$\textbf{Séquence :} \quad \frac{\{P\}\ c\ \{Q'\} \qquad \{Q'\}\ c'\ \{Q\}}{\{P\}\ c; c'\ \{Q\}}$$

$$\textbf{Test if :} \quad \frac{\{P \wedge e \neq 0\}\ c\ \{Q\} \qquad \{P \wedge e = 0\}\ c'\ \{Q\}}{\{P\}\ \textbf{if}\ e\ \textbf{then}\ c\ \textbf{else}\ c'\ \{Q\}}$$

$$\textbf{Boucle while :} \quad \frac{\{P \wedge e \neq 0\}\ c\ \{P\}}{\{P\}\ \textbf{while}\ e\ \textbf{do}\ c\ \textbf{end}\ \{P \wedge e = 0\}}$$

$$\textbf{Implication :} \quad \frac{\models (P \implies P') \qquad \{P'\}\ c\ \{Q'\} \qquad \models (Q' \implies Q)}{\{P\}\ c\ \{Q\}}$$

13.4 Développement :

On suppose donnée une fonction booléenne *even* s'évaluant à $\top$ ssi le contenu de Y est pair et on note $Y/2$ le résultat de la division euclidienne par 2 du contenu de Y.

On considère le programme suivant dans le langage jouet **IMP**.

Algorithm 5 Exponentiation rapide

```
while ¬(Y = 0) do
  while even(Y) do
    X := X × X
    Y := Y/2
  end while
  Z := Z × X
  Y := Y − 1
end while
```

Theorem . On pose c ce programme. Alors

$$\{X = m \wedge Y = n \wedge Z = 1\}\ c\ \{Z = m^n\}$$

Démonstration.

1ere Etape : Structure du programme

Examinons la structure de ce programme :

$$c = \textbf{while}\ \neg(Y = 0)\ \textbf{do}\ c'$$

où

- $c' = \textbf{while}\ even(Y)\ \textbf{do}\ c''; c'_1; c'_2$.
- $c'' = c''_0; c''_1$
- $c'_1 = Z := Z \times X$
- $c'_2 = Y := Y - 1$
- $c''_0 = X := X \times X$
- $c''_1 = Y := Y/2$

□

On a donc deux boucles **while**.

2eme Etape : Invariant

On pose $I := \{m^n = Z \times X^Y\}$ et vérifions que c'est un invariant pour la boucle **while** externe : Montrons que

$$\{I \wedge \neg(Y = 0)\}\ c'\ \{I\}$$

- D'après la règle de l'affectation, $\{I[Y \mapsto Y - 1]\}\ Y := Y - 1\ \{I\}$, ie

$$\{m^n = Z \times X^{Y-1}\}\ Y := Y - 1\ \{I\}$$

  . On pose $I' := I[Y \mapsto Y - 1]$.
- De même, $\{I'[Z \mapsto Z \times X]\}\ Z := Z \times X\ \{I'\}$.
- Par la règle de la séquence on a donc

$$\{m^n = Z \times X \times X^{Y-1}\}\ c'_1; c'_2\ \{I\}$$

- De plus, $\models (m^n = Z \times X \times X^{Y-1} \implies I)$ donc par la règle de l'implications

$$\{I\}\ c'_1; c'_2\ \{I\}$$

Montrons que I est un invariant pour la boucle interne : Encore une fois, d'après la règle de l'assignation

$$\{m^n = Z \times X^{Y/2}\}\ Y := Y/2\ \{I\}$$

et

$$\{m^n = Z \times (X \times X)^{Y/2}\}\ X := X \times X; Y := Y/2\ \{I\}$$

Or,

$$\begin{aligned} I \wedge even(Y) &\implies m^n = Z \times X^Y \wedge even(Y) \\ &\implies m^n = Z \times X^Y \wedge Y = 2 \times (Y/2) \\ &\implies m^n = Z \times X^{2\times(Y/2)} \wedge Y = 2 \times (Y/2) \\ &\implies m^n = Z \times (X^2)^{(Y/2)} \wedge Y = 2 \times (Y/2) \\ &\implies m^n = Z \times (X \times X)^{Y/2} \wedge Y = 2 \times (Y/2) \\ &\implies m^n = Z \times (X \times X)^{Y/2} \end{aligned}$$

Donc par la règle de l'implication,

$$\{I \wedge even(Y)\}\ c''\ \{I\}$$

et I est bien un invariant.

Puis par la règle du **while**

$$\{I\}\ \textbf{while}\ even(Y)\ \textbf{do}\ c''\ \{I \wedge \neg even(Y)\}$$

Comme $I \wedge \neg even(Y) \implies I$ on en déduit en appliquant la règle de conséquence

$$\{I\}\ c'\ \{I\}$$

De même, $I \wedge \neg(Y = 0) \implies I$ donc par la règle de conséquence

$$\{I \wedge \neg(Y = 0)\}\ c'\ \{I\}$$

et I est donc bien un invariant.

Par la règle du **while** on a donc

$$\{I\}\ c\ \{I \wedge \neg\neg(Y = 0)\}$$

Or,

$$\begin{aligned} X = m \wedge Y = n \wedge Z = 1 &\implies m^n = X^Y \wedge Z = 1 \\ &\implies I \end{aligned}$$

$$\begin{aligned} I \wedge \neg\neg(Y = 0) &\implies m^n = Z \times X^Y \wedge Y = 0 \\ &\implies Z = m^n \end{aligned}$$

Une dernière application de la règle d'implication donne donc le résultat

$$\{X = m \wedge Y = n \wedge Z = 1\}\ c\ \{Z = m^n\}$$

Remarque : La sémantique axiomatique (logique de Hoare) ne permet pas de prouver la terminaison : On prouve seulement une correction partielle. Par exemple ici, si $n = -1$ la boucle externe ne termine pas.

14 Une preuve formelle en logique du premier ordre

14.1 Recasages :

— 918 - Systèmes formels de preuve en logique du premier ordre. Exemples.

14.2 Références :

— [DNR03]

14.3 Prérequis :

Règles de la déduction naturelle, avec l'égalité. Les règles de l'égalité considérées sont :

$$\textbf{Introduction de l'égalité :} \quad \frac{}{\Gamma \vdash t = t} =_i$$

$$\textbf{Élimination de l'égalité :} \quad \frac{\Gamma \vdash A[t/x] \qquad \Gamma \vdash t = u}{\Gamma \vdash A[u/x]} =_e$$

De ces deux règles, on déduit que l'égalité est symétrique :

$$\dfrac{\dfrac{\dfrac{\dfrac{}{x_1 = x_2 \vdash x_1 = x_1} =_i \quad \dfrac{}{x_1 = x_2 \vdash x_1 = x_2} ax}{x_1 = x_2 \vdash x_2 = x_1} =_e}{\vdash x_1 = x_2 \to x_2 = x_1} \to_i}{\vdash \forall x_1, x_2 \{x_1 = x_2 \to x_2 = x_1\}} \forall_i$$

La règle $=_e$ a été utilisée avec $t = x_1, u = x_2$ et la formule $A[x] : x = x_1$.
On en déduit aussi des raccourcis :

$$\frac{\Gamma, u = v \vdash A[u/x]}{\Gamma, u = v \vdash A[v/x]} =_g$$

$$\frac{\Gamma, u = v, A[u/x] \vdash B}{\Gamma, u = v, A[v/x] \vdash B} ='_g$$

$$\frac{}{\Gamma, u = v \vdash t[u/x] = t[v/x]} =_c$$

14.4 Développement :

On va prouver en déduction naturelle le théorème

Theorem . Toute involution est une bijection.

L'idée dans ce développement est de traiter la preuve "mathématiques" en parallèle de la preuve formelle

Démonstration.

Preuve "papier" :

Soit f une involution. Il suffit de montrer que f est injective, et surjective (on fait le lien avec les formules).

— On commence par l'injectivité. Soit x, y ($// \forall_i$) tel que $f(x) = f(y)$ ($// \to_i$). On compose par f : $f(f(x)) = f(f(y))$ ($// =_e$). Alors puisque f est une involution, $f(f(x)) = x$ et $f(f(y)) = y$ donc $x = y$ ($//$ axiomes).

— Puis on traite la surjectivité. Soit y ($// \forall_i$). Il suffit de prouver que $f(f(y)) = y$ ($// \exists_i$). Et puisque f est une involution, $f(f(y)) = y$. ($// ax$).

□

On reformule :
On se place sur le langage $L = \{f\}$ où f est un symbole de fonction unaire.

Definition .

$$Inj : \forall x, y f(x) = f(y) \to x = y$$
$$Surj : \forall y \exists x f(x) = y$$
$$Bij : Inj \wedge Surj$$
$$Inv : \forall x, f(f(x)) = x$$

On va prouver en déduction naturelle le théorème

Theorem .

$$Inv \vdash Bij$$

$Inv \vdash Inj$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Inv, f(x) = f(y) \vdash Inv}\, ax}{Inv, f(x) = f(y) \vdash f(f(y)) = y}\, \forall_e \quad \dfrac{\pi_0}{Inv, f(x) = f(y) \vdash f(f(y)) = x}}{Inv, f(x) = f(y) \vdash x = y}\, =_e}{Inv \vdash f(x) = f(y) \to x = y}\, \to_i}{Inv \vdash Inj}\, \forall_i$$

où $=_e$ a été utilisée avec $t = f(f(y)), u = x$ et $A[z] : z = y$.
où π_0 est

$$\dfrac{\dfrac{\dfrac{}{Inv, f(x) = f(y) \vdash f(y) = f(x)}\, ax}{Inv, f(x) = f(y) \vdash f(f(y)) = f(f(x))}\, =_c \quad \dfrac{\dfrac{}{Inv, f(x) = f(y) \vdash Inv}\, ax}{Inv, f(x) = f(y) \vdash f(f(y)) = x}\, \forall_e}{Inv, f(x) = f(y) \vdash f(f(y)) = x}\, =_e$$

et la règle $=_e$ a été utilisée avec $t = f(f(x)), u = x$ et $A[z] = f(f(y)) = z$.

$Inv \vdash Surj$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{Inv \vdash Inv}\,ax}{Inv \vdash f(f(y)) = y}\,\forall_e}{Inv \vdash \{f(x) = y\}[f(y)/x]}\,\exists_i}{Inv \vdash \exists x, f(x) = y}\,\forall_i}{Inv \vdash Surj}$$

$Inv \vdash Bij$

$$\dfrac{\dfrac{\pi_1}{Inv \vdash Inj} \quad \dfrac{\pi_2}{Inv \vdash Surj}}{Inv \vdash Bij}\,\wedge_i$$

15 Algorithme de Kruskal

15.1 Recasages :

— 925 - Graphes : Représentation et algorithmes.

— 927 - Exemples de preuve d'algorithmes : Correction, terminaison.

15.2 Références :

— [CLRS02]

15.3 Developpement

Soit $G = (S, A)$ un graphe, $u \in S$ un sommet, et $E \subset A$ un ensemble d'arêtes, on note $\mathcal{C}_E(u)$ la composante connexe de u dans le graphe (S, E). Si $E = A$ on pourra ommettre l'indice.

Algorithm 6 Kruskal(G = (S, A),w)

```
E ← ∅
Trier A par ordre croissant de poids w
for (u, v) in A de poids minimal parmi les arêtes non visitées do
  if C_E(u) ≠ C_E(v) then
    E ← E ∪ {(u, v)}
  end if
end for
return E
```

Theorem . Soit $G = (S, A)$ un graphe connexe non orienté, muni d'une fonction de poids w sur les arêtes. Alors, l'algorithme de Kruskal termine et calcule un arbre couvrant de poids minimal (ACM) en temps $O(|A| \log |S|)$.

Démonstration.

Terminaison : L'algorithme traite au plus une fois chaque arête, la boucle termine en au plus $|A|$ étapes.

Correction : E est un ensemble d'arêtes. On introduit l'invariant suivant :

À chaque étape de l'algorithme, il existe T un arbre couvrant de poids minimal tq $E \subset T$

Initialisation : Au début de l'algorithme, $E = \emptyset$ donc l'invariant est trivialement vérifié.

Hérédité : Soit i une étape de la boucle, E_i la valeur de l'ensemble E à la fin de cette étape, et T_i un ACM tel que $E_i \subset T_i$. Soit (u, v) une arête de poids minimal considérée.

Dans la suite, on n'indicera pas les composantes connexes.

— Si $\mathcal{C}(u) = \mathcal{C}(v)$ alors $E_{i+1} = E_i \subset T_i$ et l'invariant est donc bien vérifié.

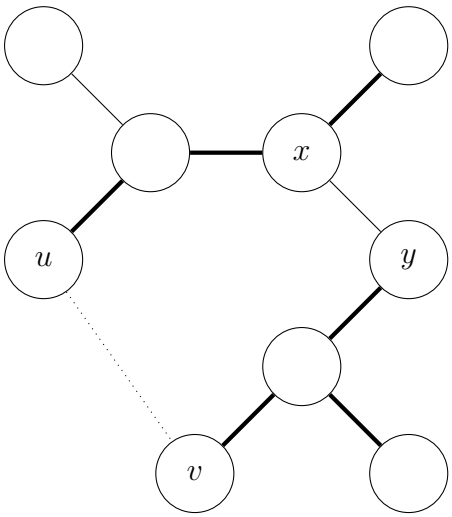
— Sinon, si $(u, v) \in T_i$ alors $E_{i+1} = E_i \cup \{(u, v)\} \subset T_i$ et l'invariant est donc bien vérifié.

— Sinon, $(\mathcal{C}(u), S - \mathcal{C}(u))$ forme une partition de S et $\mathcal{C}(v) \subset S - \mathcal{C}(u)$ (les composantes connexes sont disjointes) et $(u, v) \notin T_i$. On va construire T_{i+1} un ACM de G contenant (u, v) et tel que $E \cup \{(u, v)\} \subset T_{i+1}$.

Lemma . (u, v) crée un cycle dans T

Preuve du lemme : En effet, $u \in S(T), v \in S(T)$ et $(u, v) \notin T$. Puisque T est un arbre, il est connexe maximal, donc l'arête (u, v) crée un cycle dans T.

Comme T est un arbre, il est connexe donc il existe un chemin p reliant u à v dans T.



Puisque $v \notin \mathcal{C}(v)$ il existe au moins une arête (x, y) dans p tq $x \in \mathcal{C}(u)$ et $y \notin \mathcal{C}(u)$. On considère cette arête.

Alors $(x, y) \notin E$ et $T - \{(x, y)\}$ possède deux composantes connexes. Posons $T' := T - \{(x, y)\} + \{(u, v)\}$. Alors :

1. T' couvre S
2. T' a exactement le même nombre d'arêtes que T (ie $|S| - 1$).
3. T' est connexe : Si s, t sont deux sommets, alors il existe un chemin (dans T) de s à t.
   — Si ce chemin ne passe pas par (x, y) c'est un chemin dans T'.
   — Sinon, soit $p = p'(x, y)p''$ ce chemin. Par connexité, il existe un chemin minimal de x à u noté γ et un chemin minimal de v à y noté δ. Ces chemins ne passent pas par (x, y) par minimalité. Alors $p'\gamma(u, v)\delta p''$ est un chemin dans T' de s à t.

Montrons quil est de poids minimal :

$$w(T') = w(T) - w(x, y) + w(u, v)$$

Comme (u, v) est minimale parmi les arêtes traversant la coupe $(\mathcal{C}(u), S - \mathcal{C}(u))$ et que (x, y) traverse aussi la coupe,

$$w(u, v) \leq w(x, y)$$

et donc

$$w(T') \leq w(T)$$

Mais T' est un Arbre Couvrant, et T est de pods minimal, donc

$$w(T') \geq w(T)$$

On en déduit que

$$w(T') = w(T)$$

et T' est donc un Arbre Couvrant de Poids Minimal.

□

16 [TODO] Équivalence entre les MT et les FR

Equivalence récursive-MT

16.1 Recasages :

— 912 - Fonctions récursives primitives et non primitives. Exemples.

— 913 - Machines de Turing. Applications.

16.2 Références :

17 Complétude de la déduction naturelle

17.1 Recasages :

— 918 - Systèmes formels de preuve en logique du premier ordre. Exemples.

— 924 - Théories et modèles en logique du premier ordre.

17.2 Références :

— [Dow10]

17.3 Prérequis :

— Déduction naturelle.

— Correction de la déduction naturelle (Si $T \vdash \varphi$ alors tout modèle de T est un modèle de φ).

— L'équivalence entre les trois formes du théorème de complétude :

> **Theorem .** Soit T une théorie, et A une formule. Alors s'équivalent :
>
> (1) Si A est valide dans tous les modèles de T, alors A est démontrable dans T (ie Si $T \vDash A$ Alors $T \vdash A$)
>
> (2) Si A n'est pas démontrable dans T alors il existe un modèle de T qui n'est pas un modèle de A.
>
> (3) Si T est cohérente, alors T a un modèle (ie Si $T \nvdash \bot$ Alors $\vDash T$)

Démonstration. — (2) est la contraposée de (1) donc sont équivalentes.

— (2) implique (3) en prenant $A = \bot$.

— Supposons (3) et soit A telle que $T \nvdash A$. Alors, $T \cup \{\neg A\} \nvdash \bot$, ie $T \cup \{\neg A\}$ est cohérente. Par suite, elle a un modèle $\mathcal{M}$. Alors $\mathcal{M}$ est un modèle de T qui n'est pas un modèle de A.

□

17.4 Développement :

On va prouver la forme (3) du théorème de complétude.

Idée : Soit T une théorie cohérente. L'idée est de prendre comme modèle de M l'ensemble des termes clos, et d'interpréter les fonctions f par $\hat{f}$ qui aux termes clos $t_1, \dots, t_n$ associe le terme clos $f(t_1, \dots, t_n)$ et les prédicats P par $\hat{P}$ qui à $t_1, \dots, t_n$ associe $\top$ si la formule $P(t_1, \dots, t_n)$ est prouvable dans T et $\bot$ sinon. Cependant, ce n'est pas suffisant comme on peut le voir en considérant un langage formé d'un symbole de constante c, et de deux symboles de prédicats P, Q. Considérons de plus la théorie $T := \{P(c) \vee Q(c)\}$ formée d'un unique axiome. T est cohérente, mais le modèle ainsi construit n'est pas un modèle de T. En effet,

Lemma . $T \nvdash P(c)$

Preuve du lemme : Par correction, si $P(c)$ était prouvable, alors il serait valide, ie vrai dans tous les modèles de T. Or, si I est une interprétation telle que $[\![P(c)]\!]_I = \bot$ et $[\![Q(c)]\!]_I = \top$ alors $I \vDash T$ mais $I \nvDash P(c)$.

De même, on montre que $T \nvdash Q(c)$. Par suite, le modèle ainsi construit interprète $P(c)$ à $\bot$ et $Q(c)$ à $\bot$, et donc n'est pas un modèle de $P(c) \vee Q(c)$.

Conclusion : Il faut d'abord compléter la théorie.

Mais compléter n'est pas suffisant, car la théorie $T = \{\neg P(c), \exists x P(x)\}$ est complète, mais la construction invite à poser $\mathcal{M} = \{c\}$ et $[\![P(c)]\!]_{\mathcal{M}} = \bot$. Alors la proposition $\exists x, P(x)$ n'est pas valide dans ce modèle : Il n'y a pas de témoin qui vérifie la propriété P.

On va donc avoir en plus besoin de témoins.

Definition . Une théorie T admet des *témoins de Henkin* si lorsqu'une formule quantifiée existentiellement $\exists x \varphi$ est démontrable dans T, alors il existe un terme t tel que la formule $\varphi(t/x)$ soit démontrable dans T.

Lemma . Soit T une théorie cohérente. Si de plus T est cohérente et possède des témoins de Henkin, alors le modèle des termes clos est un modèle de T

Démonstration. On raisonne par induction sur φ pour montrer que $T \vdash \varphi$ ssi $[\![\varphi]\!]_M = \top$.

Formules atomiques C'est évident par construction de M.

Conjonction Si $T \vdash \varphi \wedge \psi$ alors via la règle $\wedge-$elim on en déduit que $T \vdash \varphi$ et $T \vdash \psi$. Par hypothèse d'induction, $[\![\varphi]\!]_M = [\![\psi]\!]_M = \top$ et donc $[\![\varphi \wedge \psi]\!]_M = \top$.
Réciproquement, on utilise la règle $\wedge-$intro.

Négation si $T \vdash \neg\varphi$ alors par cohérence $T \nvdash \varphi$. Par suite, $[\![\varphi]\!]_M = \bot$ et donc $[\![\neg\varphi]\!]_M = \top$.
Réciproquement, si $[\![\neg\varphi]\!]_M = \top$ alors $[\![\varphi]\!]_M = \bot$ donc $T \nvdash \varphi$. Par complétude, $T \vdash \neg\varphi$.

Existence On procède par équivalence, et on utilise les témoins :

$T \vdash \exists x\varphi$ ssi il existe un témoin t tel que $T \vdash \varphi(t/x)$ ssi il existe $t \in M$ tel que $[\![\varphi]\!]_M(t) = \top$ ssi $[\![\exists x\varphi]\!]_M = \top$. □

Il ne reste plus qu'à construire une extension de T qui vérifie le lemme On suppose le langage $\mathcal{L} = (\mathcal{F}, \mathcal{P})$ dénombrable. Soit H un ensemble dénombrable de constantes fraîches. Soit alors $\mathcal{L}' := (\mathcal{F} \cup H, \mathcal{P})$. $\mathcal{L}'$ est dénombrable, et on peut donc se donner une énumération φ_i des formules closes, et une énumération c_i des constantes. On construit itérativement une théorie T_i sur le langage $\mathcal{L}'$ de façon analogue à la preuve du théorème de la base incomplète :

— $T_0 = T$

— 1. Si $T_i \vdash \varphi_{i+1}$ alors on pose $\phi_{i+1} = \varphi_{i+1}$.
2. Sinon (par cohérence ces deux cas sont incompatibles), si $T_i \nvdash \varphi_{i+1}$ alors on pose $\phi_{i+1} = \not\varphi_{i+1}$.
3. On pose alors $T_{i+1} := T_i \cup \{\phi_{i+1}\}$.
4. Si de plus $\phi_{i+1} = \exists x, \psi_{i+1}$ alors on pose $T_{i+1} = T_i \cup \{\phi_{i+1}, \psi_{i+1}(t/x)\}$.

Enfin, on pose

$$T' := \cup_i T_i$$

Alors :

T' est cohérente : Par récurrence, toutes les T_i sont cohérentes : C'est le cas par hypothèse pour $i = 0$. Supposons T_i cohérente.

1. Si $T_i \vdash \varphi_{i+1}$ alors dire que $T_{i+1} \vdash \bot$ revient à $T_i, \varphi_{i+1} \vdash \bot$ donc $T_i \vdash \bot$ en remplaçant chaque règle axiome (pour φ_{i+1}) par une preuve de φ_{i+1}. C'est absurde.
2. De même, si $T_i \nvdash \varphi_{i+1}$ alors si $T_{i+1} \vdash \bot$, on a $T_i, \neg\varphi_{i+1} \vdash \bot$, alors la dernière règle utilisée dans cette dérivation est $\neg-$elim, et par suite $T_i, \neg\varphi_{i+1} \vdash \varphi_{i+1}$ et donc $T_i \vdash \varphi_{i+1}$. Par suite, $T_i \vdash \bot$. Absurde.
3. Si $T_i \vdash \exists x, \phi$, et si T_{i+1} est incohérente alors $T_i, (c_{i+1}/x)\phi \vdash \bot$. Par la règle $\exists-$elim on en déduit que $T_i \vdash \bot$.

Donc s'il existe une démonstration de $\bot$ dans la théorie T', cette dérivation formerait un arbre fini, donc il existerait un sous ensemble fini $\phi_1, \ldots, \phi_n$ de T' tel que $\phi_1, \ldots, \phi_n \vdash \bot$ soit démontrable dans T'. On peut inclure cet ensemble fini dans un certain T_i, ce qui nierait la cohérence de T_i.

T' est complète Soit A une formule quelconque. Alors il existe i telle que $\varphi_i = A$. Donc A ou $\neg A$ est un axiome, et par suite $T \vdash A$ ou $T \vdash \neg A$.

T' a des témoins de Henkin Si la proposition $\exists x, \phi$ est démontrable dans T' alors il existe i tel que φ_i

Conclusion :

La théorie T' ainsi construite a donc un modèle, qui est aussi un modèle de T par restriction du langage !

17.5 Postrequis :

— *Pourquoi il ne suffit pas de prendre les termes clos comme modèle, en interprétant les fonctions f par $\hat{f}$ qui aux termes clos $t_1, \ldots, t_n$ associe le terme clos $f(t_1, \ldots, t_n)$ et les prédicats P par $\hat{P}$ qui à $t_1, \ldots, t_n$ associe $\top$ si la formule $P(t_1, \ldots, t_n)$ est prouvable dans T et $\bot$ sinon. ?* $\rightarrow$ Considérons un langage formé d'un symbole de constante c, et de deux symboles de prédicats P, Q. Considérons de plus la théorie $T := \{P(c) \vee Q(c)\}$ formée d'un unique axiome. T est cohérente, mais le modèle ainsi construit n'est pas un modèle de T. En effet,

—

18 Arithmétique de Presburger

18.1 Recasages :

— 909 - Langages rationnels et Automates finis. Exemples et applications.
— 914 - Décidabilité et indécidabilité. Exemples.
— 924 - Théories et modèles en logique du premier ordre. Exemples.

18.2 Références :

— Adapté depuis [Car14], avec un peu de [DNR03] pour les définitions.

18.3 Prérequis :

— Manipulation d'automates et de formules logiques du premier ordre.
— Propriétés de clotures "Effectives"

Definition . La théorie d'une structure $\mathcal{M}$ est $Th(\mathcal{M}) := \{\varphi \text{Formule close} \mid \mathcal{M} \vDash \varphi\}$

18.4 Développement :

Theorem . Le problème suivant est décidable :
DONNÉE φ une formule close du premier ordre sur la signature $\{0, 1, +, =\}$.
QUESTION φ est valide dans $\mathbb{N}$?

Démonstration.

Idée :
On va construire un codage des valuations de sorte que l'ensemble des codages de valuations qui satisfont une formule forment un langage rationnel, dont on sait construire un automate.

Puisque φ est close, il suffira de tester si le langage associé est vide (auquel cas aucune valuation ne satisfait φ et $\mathbb{N} \nvDash \varphi$), ou bien si c'est le langage formé du seul mot vide (auquel cas la valuation vide satisfait φ et donc $\mathbb{N} \vDash \varphi$).

Codage :

Posons $\Sigma = \{0, 1\}$. Si $n \in \mathbb{N}^\star$, notons $bin(n) \in \Sigma^*$ l'unique représentation binaire de n avec bit de poids fort à droite, qui termine par un 1. On posera de même $bin(0) = \varepsilon$. Si $n_1, \ldots, n_k \in \mathbb{N}$ on désigne par $[n_1, \ldots, n_k]$ un codage de $bin(n_1), \ldots, bin(n_k)$ sur l'alphabet Σ^k, en rajoutant des 0 dans les trous. Ce codage est unique étant donné un tuple, modulo les 0 non significatifs à droite.

Exemple : $[18, 7, 6]$ est codé par $(0,1,0)(1,1,1)(0,1,1)(0,0,0)(1,0,0)$.

Si $\varphi(x_1, \ldots, x_m)$ est une formule avec $fv(\varphi) \subset \{x_1, \ldots, x_m\}$, on va construire (par induction structurelle) un automate A_φ sur l'alphabet σ^m tel que

$$\mathcal{L}(A_\varphi) = \{[n1, \ldots, n_m] \mid \mathbb{N} \vDash \varphi(n_1, \ldots, n_m)\}$$

Enrichissement de l'alphabet :

On commence par prouver qu'on peut enrichir l'alphabet de travail

> **Theorem .** Si $fv(\varphi) \subset \nu \subsetneq \nu'$ et si A_φ est un automate pour φ sur $\Sigma^{|\nu|}$ alors on peut construire un automate sur $\Sigma^{|\nu'|}$ pour φ.

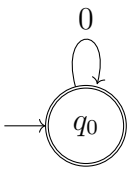
Démonstration. On considère le morphisme alphabétique

$$f : \begin{cases} (\Sigma^{|\nu'|})^\star & \to & (\Sigma^{|\nu|})^\star \\ (a_x)_{x \in \nu'} & \mapsto & (a_x)_{x \in \nu} \end{cases}$$

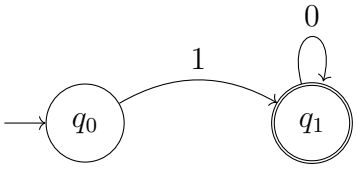
Alors, $f^{-1}(\mathcal{L}(A_\varphi))$ est reconnaissable (cloture par morphisme inverse), et on peut construire un automate sur $\Sigma^{|\nu'|}$ le reconnaissant. □

Cas de base :

— Pour $x = 0$

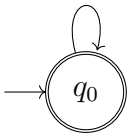


— Pour $x = 1$

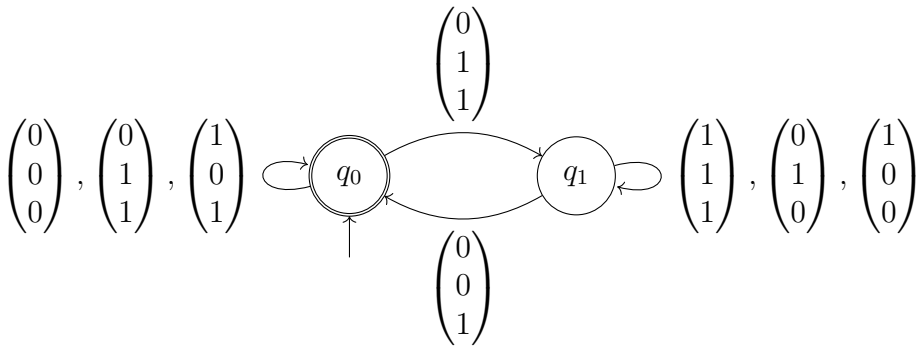


— Pour $x = y$:

$$\binom{0}{0}, \binom{1}{1}$$



— Pour $x = y + z$:



Induction :

— Si $\varphi = \neg\varphi'$ on construit un automate pour φ', on le déterminise, et on en prend le complémentaire.

— Si $\varphi = \varphi_1 \wedge \varphi_2$, on construit deux automates A_{φ_1} et A_{φ_2} sur $fv(\varphi_1) \bigcup fv(\varphi_2)$ pour φ_1, φ_2 à l'aide du lemme d'enrichissement. Alors, l'automate produit $A_{\varphi_1} \bigcap A_{\varphi_2}$ reconnaît les valuations satisfaisant $\varphi_1 \wedge \varphi_2$.

— Si $\varphi = \exists x_i \phi$ alors considérons un automate pour ϕ :

$$A_\phi = (Q, \Sigma^{|fv(\phi)|}, I, T, F)$$

Par projection on construit

$$A_{\exists x_i \phi} := (Q, \Sigma^{|fv(\phi)|}, I, T', F)$$

avec

$$\text{Si } (q, \begin{pmatrix} c_1 \\ \vdots \\ c_{i-1} \\ c_i \\ c_{i+1} \\ \vdots \\ c_n \end{pmatrix}, q') \in T, \quad \text{Alors } (q, \begin{pmatrix} c_1 \\ \vdots \\ c_{i-1} \\ c_{i+1} \\ \vdots \\ c_n \end{pmatrix}, q') \in T'$$

Finalement, pour décider la validité d'une formule close φ, on construit sont automate A_φ et on vérifie si son langage est non vide. Ceci se résume donc à un problème d'accessibilité d'un état final depuis un état initial dans le graphe de l'automate.

□

18.5 Postrequis

— La complexité prend des tournures exponentielles à cause des déterminisations pour prendre le complémentaire (négation d'une formule). Voir [DGH10] pour une preuve de complexité triple exponentielle.

19 Complexité du tri rapide avec pivot aléatoire

19.1 Recasages :

— 903 - Exemples d'algorithmes de tri. Exemples et applications.
— 926 - Analyse des algorithmes : complexité. Exemples.

19.2 Références :

— [CLRS02]

19.3 Developpement

Theorem . On considère l'algorithme du tri rapide avec choix du pivot aléatoire. Alors il effectue dans le pire des cas $O(n^2)$ opérations, mais $O(n \log n)$ en moyenne .

Démonstration. Soit T un tableau à n éléments. On supposera que le pivot est tiré selon une loi uniforme, de façon indépendante et que tous les éléments sont distincts. Si les éléments ne sont pas distincts, il suffit de faire une première lecture du tableau et de marquer chaque élément par son indice dans le tableau (On remplace $T[i]$ par le couple $(T[i], i)$). On peut alors réaliser un tri rapide en utilisant l'ordre lexicographique. Ceci a l'avantage d'obtenir un tri en place.

Pire cas : Soit $P(n)$ le nombre de comparaisons dans le pire des cas sur une entrée de taille n. TRI-RAPIDE partage ce tableau en deux sous tableaux de tailles k et $n-1-k$ en effectuant $n-1$ comparaisons. On en déduit donc

$$P(n) = \max_{0 \leq k \leq n-1} (P(k) + P(n-1-k)) + n - 1$$

On raisonne par substitution : S'il existe une constante c telle que $P(j) \leq cj^2$ pour $j < n$. Alors

$$\begin{aligned} P(n) &\leq \max_{0 \leq k \leq n-1} (ck^2 + c(n-1-k)^2) + n - 1 \\ &= c \max_{0 \leq k \leq n-1} (k^2 + (n-1-k)^2) + n - 1 \end{aligned}$$

Or, par convexité, $k \mapsto k^2 + (n-1-k)^2$ atteint son maximum sur l'extémité de cet intervalle. On en déduit que

$$\max_{0 \leq k \leq n-1} k^2 + (n-1-k)^2 \leq (n-1)^2$$

Finalement

$$P(n) \leq cn^2 - c(2n-1) + n - 1 \leq cn^2$$

en choisissant c convenablement.

Donc $P(n) = O(n^2)$. Et cette complexité est atteinte lorsque le partionnement est totalement déséquilibré (pivot choisi comme le plus petit élément).

Cas moyen :

— Chaque appel de PARTITION selection un pivot à qui sont comparés tous les éléments du segment. Ce pivot ne figurera plus jamais dans les appels récursifs ultérieurs. Il y a donc au plus n appels à PARTITION.

— Dans chaque itération de la boucle FOR de partition, on fait exactement 1 comparaison de l'élément pivot à 1 autre élément.

Soit X le nombre total de comparaisons lors du tri de T. Soit $[z_1, \dots, z_n]$ l'ensemble des éléments de T ordonnés selon l'ordre final. On pose $Z_{i,j} := [z_i, \dots, z_j]$ pour $i \leq j$ le sous intervalle.

Lemma . Chaque paire $\{z_i, z_j\}$ est comparée au plus une fois.

Preuve du lemme : z_i est comparé à z_j ssi l'un des deux est le pivot. Or, le pivot n'apparaît dans aucun sous tableau utilisé dans les appels récursifs. Donc la comparaison a lieu au plus une fois.

Notons $A_{i,j}$ l'événement $\{z_i \text{ est comparé à } z_j\}$ et posons $X_{i,j} := \mathbb{1}_{A_{i,j}}$. Alors

$$X = \sum_{i<j} X_{i,j}$$

et par linéarité,

$$\mathbb{E}X = \sum_{i<j} \mathbb{P}(A_{i,j})$$

Considérons alors deux cas :

Si un pivot x est selectionné tel que $z_i < x < z_j$: Alors z_i et z_j seront comparés à x, puis placés dans deux sous tableaux distincts. Ils ne seront donc *jamais* comparés.

Si z_i (respectivement z_j) est choisi comme pivot avant tout autre élément de $Z_{i,j}$: Alors z_i (resp. z_j) sera comparé à tous les éléments de $Z_{i,j}\backslash\{z_i\}$ (resp. $Z_{i,j}\backslash\{z_j\}$).

Ainsi, z_i est comparé à z_j ssi l'un des deux est le premier élément de $Z_{i,j}$ à être choisi comme pivot. Par suite :

$$\begin{aligned}
\mathbb{P}(A_{i,j}) &= \mathbb{P}(z_i \text{ ou } z_j \text{ est le premier pivot de } Z_{i,j}) \\
&= \mathbb{P}\left(\{z_i \text{ est le premier pivot de } Z_{i,j}\} \bigsqcup \{z_i \text{ est le premier pivot de } Z_{i,j}\}\right) \\
&= \mathbb{P}(z_i \text{ est le premier pivot de } Z_{i,j}) + \mathbb{P}(z_j \text{ est le premier pivot de } Z_{i,j}) \\
&= \frac{2}{j-i+1}
\end{aligned}$$

On a donc

$$\begin{aligned}
\mathbb{E}X &= \sum_{i<j} \frac{2}{j-i+1} \\
&= \sum_{i=1}^{n-1} \sum_{k=1}^{n-i} \frac{2}{k+1} \\
&\leq \sum_{i=1}^{n-1} \sum_{k=1}^{n} \frac{2}{k} \\
&\leq 2 \sum_{i=1}^{n-1} H_n \\
&\leq 2nH_n
\end{aligned}$$

On en déduit que $\mathbb{E}X = O(n \log n)$. □

19.4 Postrequis

On peut de la même façon obtenir la variance par indépendance.

20 Complétude réfutationnelle de la résolution propositionnelle

20.1 Recasages :

— 916 - Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications.

20.2 Références :

— Adapté depuis le Goubault [GLM97]

20.3 Prérequis

— Formes normales, NNF, CNF

— Calcul des séquents propositionnel $\mathbf{LK_0}$ + coupure : Correction, complétude du système de preuve.

— Réfutation ; une formule est valide ssi sa négation est insatisfiable

20.4 Développement

On se donne une formule φ sous forme CNF :

$$\varphi := \bigwedge_{i=1}^{n} C_i$$

. On note $S(\varphi) := \{C_1, \ldots, C_n\}$ l'ensemble des clauses de φ.

La seule règle de résolution est la règle de coupure.

$$\frac{C \vee l_i \qquad C' \vee \neg l_i}{C \vee C'}$$

L'idée est de procéder par saturation. On note $R(\varphi)$ l'ensemble des clauses dériables à partir de $S(\varphi)$ via la règle de résolution.

> **Theorem .** φ est insatisfaisable si et seulement si $\bot \in R(\varphi)$

Le sens réciproque provient de la correction du calcul des sequents, donc en particulier de la règle de coupure : Si $\bot \in R(\varphi)$ alors φ n'a aucun modèle. Donc en particulier est insatisfaisable. Le but de ce développement est donc de prouver le sens direct.

20.5 Preuve :

⚠ Attention : La preuve telle quelle est trop longue. Il faut mettre la définition de l'arbre sémantique dans le plan, et la définition d'une interprétation partielle. Dans ce développement, ne faire que les étapes 1 à 3 + un exemple pour rappeler les définitions du plan.

Preuve : Supposons φ insatisfiable. Alors puisque $S(\varphi) \subset R(\varphi)$ il est clair que $R(\varphi)$ reste insatisfiable. On va utiliser une méthode dite des arbres sémantiques.

Definition . Si I est une interprétation partielle et φ une formule propositionnelle. On dit que $I \vDash \varphi$ s'il existe I' une interprétation totale étendant I et telle que $I \vDash \varphi$

Definition . Soit S un ensemble fini de clauses [a]. Soit $\mathcal{P}_0(S)$ l'ensemble des variables propositionnelles qui apparaissent dans S. $\mathcal{P}_0$ est fini. On se fixe une énumération injective (A_i) de ces variables propositionnelles.

On construit un arbre binaire (fini) étiqueté par des interprétations partielles de S de la façon suivante :

- La racine est étiquetée par l'interprétation de domaine vide.
- L'étage $i \leq n$ est étiqueté par la variable A_i
- Le noeud i correspond à une interprétation partielle de S dans laquelle on n'interprète que les variables d'indice $< i$.
- Pour tout noeud étiqueté par l'interprétation partielle I, et d'étage P, le fils gauche est associé à I étendu par $I[\bot/P]$ et le fils droit à I étendu par $I[\top/P]$.

On appelle cet arbre, arbre sémantique pour S.

a. Notre formule ne posède qu'un nombre fini de clauses, donc c'est ok. Si on pose la question pour un nombre infini, on sort un argument de compacité qu'on peut prouver indépendamment, via tychonoff par exemple. Si le jury semble bougon, on explique rapidement la preuve de compacité par les arbres Sémantiques. Le mot clef est théorème de König.

Insérer un dessin d'arbre sémantique pour $S = \{B, A \vee \neg B, \neg A \vee C, \neg C\}$

Definition .

- On appelle *Noeud d'échec* tout noeud qui correspond à une interprétation ne satisfaisant pas une clause de S.
- On appelle *Noeud d'inférence* tout noeud dont les deux fils sont des noeuds d'échec.
- On appelle arbre sémantique clos d'un ensemble de clauses S l'arbre binaire obtenu en élaguant l'arbre sémantique de S à chaque noeud d'échec.

L'idée du théorème est alors de procéder par rafinement de l'arbre sémantique clos de $S(\varphi)$ en appliquant judicieusement la règle de résolution, puis en élagant l'arbre obtenu à chaque étape, jusqu'à obtenir l'arbre sémantique clos réduit à la clause vide $\bot$.

1ere étape : Finitude des arbres sémantiques clos $S(\varphi)$ est insatisfiable, donc son arbre sémantique ne possède que des noeuds d'échec. En particulier, son arbre sémantique clos ne possède pas de branche infinie. Puisque c'est un arbre binaire, le lemme de König permet de conclure à la finitude de l'arbre sémantique de $S(\varphi)$.

Par ailleurs, si B est un ensemble de clauses obtenues à partir de A par résolution propositionnelle, alors $A \subset B$ et les variables propositionnelles présentes dans B sont celles présentes dans A. On en déduit que l'arbre sémantique de B est un sous-arbre de l'arbre sémantique de A, de même pour les arbres sémantiques clos.

Donc finalement, l'arbre sémantique clos obtenu à chaque étape est fini d'une part, et de taille (= nombre de noeuds) décroissante.

2ème étape : Lemme technique

Factoriser cette preuve

Lemma . Soit T un arbre sémantique clos à n noeuds. Si la racine n'est pas un noeud d'échec, alors T possède au moins un noeud d'inférence.

Démonstration. Soit T un tel arbre sémantique. Puisque la racine n'est pas un noeud d'echec, alors $n \geq 3$. On va résonner par récurrence sur n.

- Si $n = 3$ alors la racine est un noeud d'inférence.
- Si $n > 3$ alors la racine n'est pas un noeud d'échec, et possède au moins un fils qui n'est pas un noeud d'échec. Ce noeud enracine un arbre à au moins 3 noeuds, et au plus $n-2$. Donc par hypothèse d'induction, il possède un noeud d'inférence, qui est alors un noeud d'inférence de T.

□

3ème étape : Résolution propositionnelle On va de nouveau résonner par induction sur le nombre n de noeuds de l'arbre sémantique clos de $S(\varphi)$.

- Si $n = 1$ alors $S(\varphi) = \{\bot\}$ donc $\bot \in R(\varphi)$.
- Supposons $n > 1$. Alors la racine n'est pas un noeud d'échec. Par le lemme précédent, l'arbre possède un noeud d'inférence étiqueté par une interprétation partielle I, à l'étage étiqueté par la variable propositionnelle P. Ses deux fils sont donc des noeuds d'échec associés à deux clauses C_1, C_2. On va voir qu'on peut appliquer la résolution à C_1, C_2 en utilisant P. En effet,

$$I[\bot/P] \not\models C_1 \quad \text{et} \quad I[\top/P] \not\models C_2$$

Mais comme ce noeud d'inférence n'est pas un noeud d'échec, $I \models C_1$ et $I \models C_2$. Ainsi, il existe un littéral dans C_1 satisfait par I mais pas par $I[\bot/P]$. Nécessairement $C_1 = C_1' \vee P$. De même, nécessairement $C_2 = C_2' \vee \neg P$. Par résolution, $\{C_1, C_2\} \vdash C := C_1', C_2'$ et donc $S(\varphi) \vdash C$ par résolution. On observe alors que $I \not\models C$ [1]. Ainsi, en considérant $I' \subset I$ minimale telle que $I'\neg \models C$, et en élaguant à I', on obtient un n noeud d'échec dans l'arbre sémantique clos de $S(\varphi) \cup \{C\}$. Par hypothèse d'induction, $S(\varphi) \cup \{C\} \vdash^* \bot$ par résolution, et donc $\bot \in R(\varphi)$.

1. Sinon sans perte de généralité $I \models C_1'$. Comme $P \notin C_1'$ on en déduit que $I[\bot/P] \models C_1'$ et donc $I[\bot/P] \models C_1' \vee P = C_1$ ce qui est absurde par hypothèse.

Conclusion : On a donc prouvé qu'une formule φ était insatisfaisable, ssi on pouvait dériver $\bot$ par résolution. On a même fait mieux puisqu'en dessinant l'arbre sémantique clos de φ on sait immédiatement où faire les résolutions successives : C'est à chaque noeud d'inférence !

□

20.6 Postrequis

Postrequis pour la résolution propositionnelle : Compacité ? Premier ordre ?

— Si on considère des arbres sémantiques infinis, on peut déduire du lemme de König le théorème de compacité, et appliquer la résolution à un ensemble infini de clauses.

— Le nombre de résolutions nécessaires pour dériver $\bot$ est majoré par le nombre de noeuds d'inférences dans l'arbre clos de $S(\varphi)$, donc majoré par 2^n.

— Si comme pour le premier ordre on considère plutôt des multi ensembles de clauses, il est necessaire de rajouter une règle de contraction/factorisation et de l'utiliser pour n'obtenir qu'un seul littéral pour réfuter une clause à l'étape 3.

21 Adéquation de la sémantique dénotationnelle par rapport à la sémantique opérationnelle

21.1 Recasages :

— 930 - Sémantique des langages de programmation. Exemples.

21.2 Références :

[Win93] et http://www.lsv.fr/~goubault/CoursProgrammation/prog1_sem2.pdf

21.3 Prérequis :

— Théorème de correction de la sémantique dénotationnelle par rapport à la sémantique opérationnelle.

— Théorème d'adéquation pour les expressions arithémtiques et les booléens.

Sémantique opérationnelle (à grands pas) :

$$\frac{}{\langle \mathbf{skip}, \sigma\rangle \to \sigma}$$

$$\frac{\langle a, \sigma\rangle \to m}{\langle X := a, \sigma\rangle \to \sigma[X \mapsto m]}$$

$$\frac{\langle c_0, \sigma\rangle \to \sigma'' \qquad \langle c_1, \sigma''\rangle \to \sigma'}{\langle c_0; c_1, \sigma\rangle \to \sigma'}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{true} \qquad \langle c_0, \sigma\rangle \to \sigma'}{\langle \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1, \sigma\rangle \to \sigma'}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{false} \qquad \langle c_1, \sigma\rangle \to \sigma'}{\langle \mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1, \sigma\rangle \to \sigma'}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{false}}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma\rangle \to \sigma}$$

$$\frac{\langle b, \sigma\rangle \to \mathbf{true} \qquad \langle c, \sigma\rangle \to \sigma'' \qquad \langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma''\rangle \to \sigma'}{\langle \mathbf{while}\, b\, \mathbf{do}\, c, \sigma\rangle \to \sigma'}$$

Sémantique dénotationnelle des commandes

On fait des fonctions partielles, j'pense que c'est plus clair, ça c'est les notations du Winskell

La sémantique dénotationnelle d'une commande est une fonction partielle de signature $\Sigma \to \Sigma$, qu'on représente à l'aide de son graphe $\{(\sigma, \sigma') \mid \sigma \in dom[\![c]\!] \wedge [\![c]\!]\sigma = \sigma'\}$. La sémantique dénotationnelle des opérations arithmétiques et booléennes sont des fonctions totales.

$$[\![\mathbf{skip}]\!] = \{(\sigma, \sigma) \mid \sigma \in \Sigma\}$$

$$[\![X := a]\!] = \{(\sigma, \sigma[X \mapsto n]) \mid \sigma \in \Sigma \wedge n = [\![a]\!]\sigma\}$$

$$[\![c_0; c_1]\!] = [\![c_0]\!] \circ [\![c_1]\!]$$

$$\begin{aligned}[\![\mathbf{if}\, b\, \mathbf{then}\, c_0\, \mathbf{else}\, c_1]\!] = &\{(\sigma, \sigma') \mid [\![b]\!] = \mathbf{true} \wedge (\sigma, \sigma') \in [\![c_0]\!]\} \cup \\ &\{(\sigma, \sigma') \mid [\![b]\!] = \mathbf{false} \wedge (\sigma, \sigma') \in [\![c_1]\!]\}\end{aligned}$$

$$[\![\mathbf{while}\, b\, \mathbf{do}\, c_0]\!] = \mathrm{lfp}(\Gamma)$$

où

$$\begin{aligned}\Gamma(\varphi) = &\{(\sigma, \sigma') \mid [\![b]\!]\sigma = \mathbf{true} \wedge (\sigma, \sigma') \in \varphi \circ [\![c_0]\!]\} \\ &\cup \{(\sigma, \sigma) \mid [\![b]\!]\sigma = \mathbf{false}\}\end{aligned}$$

21.4 Développement

Theorem . Pour toute commande c,

$$(\sigma, \sigma') \in [\![c]\!] \implies \langle c, \sigma\rangle \to \sigma'$$

Remarque : Le théorème d'adéquation est un théorème de terminaison : Si la sémantique dénotationnelle de c est bien définie sur l'entrée σ et vaut $\sigma' \neq \bot$ alors le programme c doit nécessairement terminer sur l'entrée σ avec pour résultat σ'.

Démonstration. La preuve se fait par induction structurelle sur c.

$c \equiv \mathbf{skip}$ **:** Par définition $[\![\mathbf{skip}]\!]\sigma = \sigma'$ pour tout σ. Ainsi, si $(\sigma, \sigma') \in [\![\mathbf{skip}]\!]$ alors $\sigma' = \sigma$ et par suite $\langle \mathbf{skip}, \sigma\rangle \to \sigma'$.

$c \equiv X := a$ **:** Si $(\sigma, \sigma') \in [\![X := a]\!]$. Alors $\sigma' = \sigma[X \mapsto n]$ où $n = [\![a]\!]\sigma$. Par le théorème d'adéquation pour les opérateurs arithmétiques, $\langle a, \sigma\rangle \to n$ et donc $\langle c, \sigma\rangle \to \sigma'$ par la règle de l'affectation dans la sémantique opérationnelle.

$c \equiv c_0; c_1$ **:** Si $(\sigma, \sigma') \in [\![c_0; c_1]\!]$. Alors il existe σ'' tel que $(\sigma, \sigma'') \in [\![c_0]\!]$ et $(\sigma'', \sigma') \in [\![c_1]\!]$. Par l'hypothèse d'induction structurelle, $\langle c_0, \sigma\rangle \to \sigma''$ et $\langle c_1, \sigma''\rangle \to \sigma'$. Donc par la règle de la séquence, $\langle (c_0; c_1), \sigma\rangle \to \sigma'$.

$c \equiv \textbf{if}\, b\, \textbf{then}\, c_0\, \textbf{else}\, c_1$ **:** Soit $(\sigma, \sigma') \in [\![c]\!]$. On sépare deux cas :

(i) Si $[\![b]\!]\sigma = \textbf{true}$ alors $(\sigma, \sigma') \in [\![c_0]\!]$. Par le théorème d'adéquation pour les expressions booléennes, on en déduit que $\langle b, \sigma\rangle \to \textbf{true}$ et par l'hypothèse d'induction structurelle, $\langle c_0, \sigma\rangle \to \sigma'$, et donc par la règle de branchement conditionnel **true** on en déduit que $\langle c, \sigma\rangle \to \sigma'$.

(ii) De même, si $[\![b]\!]\sigma = \textbf{false}$ alors $\langle b, \sigma\rangle \to \textbf{false}$. Par ailleurs, $(\sigma, \sigma') \in [\![c_1]\!]$ donc par l'hypothèse d'induction structurelle, $\langle c_1, \sigma\rangle \to \sigma'$. Par la règle de branchement conditionnel **false**, on en déduit que $\langle c, \sigma\rangle \to \sigma'$.

Dans les deux cas, l'hypothèse d'induction est valide.

$c \equiv \textbf{while}\, b\, \textbf{do}\, c_0$ **:** Par l'hypothèse d'induction structurelle, pour tout environnement $(\sigma, \sigma') \in [\![c_0]\!]$ alors $\langle c_0, \sigma\rangle \to \sigma'$. Rappelons que la sémantique du **while** est le plus petit point fixe de Γ. Posons $\theta_n = \Gamma^n(\emptyset)$, de sorte que

$$\begin{aligned}\theta_0 &= \emptyset \\ \theta_{n+1} &= \{(\sigma, \sigma') \mid [\![b]\!]\sigma = \textbf{true} \wedge (\sigma, \sigma') \in \theta_n \circ [\![c_0]\!]\} \cup \\ &\quad \{(\sigma, \sigma) \mid [\![b]\!]\sigma = \textbf{false}\}\end{aligned}$$

On a alors

$$[\![c]\!] = \bigcup_{n \in \mathbb{N}} \theta_n$$

Prouvons par récurrence sur n que

$$\forall \sigma, \sigma' \in \Sigma, (\sigma, \sigma') \in \theta_n \implies \langle c, \sigma\rangle \to \sigma'$$

Initialisation : Le résultat est vrai par $n = 0$ (on quantifie universellement sur l'ensemble vide).

Hérédité : Supposons le résultat vrai pour $n \in \mathbb{N}$. Soit $(\sigma, \sigma') \in \theta_{n+1}$.

Si $[\![b]\!]_\sigma = \textbf{true}$ et $(\sigma, \sigma') \in \theta_n \circ [\![c_0]\!]$ Alors $\langle b, \sigma\rangle \to \textbf{false}$. Par ailleurs, il existe σ'' tel que $(\sigma, \sigma'') \in [\![c_0]\!]$ et $(sigma'', \sigma') \in \theta_n$. Par l'hypothèse de récurrence, on en déduit que $\langle c, \sigma''\rangle \to \sigma'$. Par l'hypothèse d'induction structurelle sur le programme on a aussi $\langle c_0, \sigma\rangle \to \sigma''$. Par la règle du **while** on a donc finalement $\langle c, \sigma\rangle \to \sigma'$.

Sinon, $[\![b]\!]_\sigma = \textbf{false}$ et $\sigma' = \sigma$ On en déduit que $\langle b, \sigma\rangle \to \textbf{false}$ et $\langle c, \sigma\rangle \to \sigma$ ie $\langle c, \sigma\rangle \to \sigma'$. □

21.5 Conclusion :

On a bien prouvé le théorème d'adéquation de la sémantique dénotationnelle vis à vis de la sémantique opérationnelle à grands pas.

21.6 Postrequis :

Postrequis sémantique

— Théorème de correction ?

22 Tri par dénombrement et tri par base.

22.1 Recasages :

— 903 - Exemples d'algorithmes de tri. Correction et complexité.

22.2 Références :

— [CLRS02]

22.3 Developpement :

Algorithm 7 Tri-Dénombrement(A, k)

Input: A un tableau d'entiers dans $\{0, \dots, k\}$ à trier, et l'entier k.

```
n := |A|
Allouer B de taille n
Allouer C de taille k + 1 rempli de 0
for j = 0 to n − 1 do
    C[A[j]] := C[A[j]] + 1
end for
for i = 1 to k do
    C[i] := C[i] + C[i − 1]
end for
for j = n to 1 do
    B[C[A[j]]] := A[j] ;
    C[A[j]] := C[A[j]] − 1 ;
end for
return B
```

Algorithm 8 Tri-Base(A, d, k)

Input: A un tableau d'entiers à trier, d un nombre de chiffres, k une base.

```
for i = 1 to d do
    Trier par dénombrement A selon le chiffre i, avec la base k.
end for
return A
```

Theorem Correction et Stabilité. Le tableau B renvoyé par l'algorithme du tri par dénombrement est trié, et il s'agit d'un tri stable.

Theorem Complexité. L'algorithme fonctionne en temps $O(n + k)$

Theorem . Le tableau renvoyé par l'algorithme du tri par base est trié en temps $O(d(n+k))$.

22.4 Preuve

On commence par donner l'exemple du Cormen pour le tri par dénombrement.

Preuve de correction. On commence par les deux remarques suivantes :

— À la fin de la première boucle, $C[i]$ contient le nombre d'éléments égaux à i :

$$C[i] = |\{j \mid j \in \{1,\dots,n\} \wedge A[j] = i\}|$$

— À la fin de la deuxième boucle, $C[i]$ contient le nombre d'éléments inférieurs ou égaux à i.

Il ne reste plus qu'à placer chaque élément $A[j]$ à sa bone place dans le tableau de sortie B : $A[j] \leq A[j]$ mais $A[j] > A[j]-1$ donc il doit être placé dans l'intervalle $\{C[A[j]-1]+1,\dots,C[A[j]]\}$.

On utilise l'invariant suivant :

Au tour de boucle j,

$$C[i] = |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' > j \mid j' \in \{1,\dots,n\} \wedge A[j'] = i\}|$$

— Avant la boucle, le deuxième ensemble est vide, et donc $C[i] = |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}|$ ce qui est assuré par la deuxième boucle.

— Supposons que le résultat soit vrai pour $j \geq 2$ en début de boucle. Prouvons qu'au début du prochain tour de boucle l'invariant est toujours vérifié :

— Pour $i \in \{0,\dots,k\}\backslash\{A[j]\}$, $C[i]$ n'est pas modifié, donc

$$\begin{aligned} C[i] &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' > j \mid j' \in \{1,\dots,n\} \wedge A[j'] = i\}| \\ &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' \geq j \mid j' \in \{1,\dots,n\} \wedge A[j'] = i\}| \\ &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' > j-1 \mid j' \in \{1,\dots,n\} \wedge A[j'] = i\}| \end{aligned}$$

— Pour $i = A[j]$. Alors, $C[i]$ est décrémenté de 1 :

$$\begin{aligned} C[i] &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' > j \mid j' \in \{1,\dots,n\} \wedge A[j'] = i\}| - 1 \\ &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - (|\{j' > j \mid j' \in \{1,\dots,n\} \wedge A[j'] = A[j]\}| + 1) \\ &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' \geq j \mid j' \in \{1,\dots,n\} \wedge A[j'] = A[j]\}| \\ &= |\{j' \mid j' \in \{1,\dots,n\} \wedge A[j'] \leq i\}| - |\{j' > j-1 \mid j' \in \{1,\dots,n\} \wedge A[j'] = i\}| \end{aligned}$$

et comme j est décrémenté, c'est vrai au prochain tour de boucle.

Cet invariant étant vérifié, à tout moment on a $C[A[j]]$ est la position finale de $A[j]$. Soit $j_1 > j_2$ tels que $A[j_1] = A[j_2]$. Alors, puisque l'on décrémente $C[A[j]]$, on en déduit que $A[j_2]$ est placé à gauche de $A[j_1]$. Donc le tri est stable.

□

Complexité. — La construction de B se fait en temps n.

— La construction de C se fait en temps k.

— Les trois boucles fonctionnent en temps k ou n.

Donc l'algorithme fonctionne en $O(k+n)$. Dans le cas où $k = O(n)$, on a même une complexité en $O(n)$. □

Correction tri par base. On raisonne par récurrence sur le nombre i de chiffres triés (ie sur la colonne en cours, la colonne 0 étant la colonne des unités). Pour la simplicité, on suppose que les entiers ont tous d chiffres, quitte à rajouter des 0 non significatifs. On va donc prouver que les éléments tronqués au ie chiffre sont triés.

— Quand aucun chiffre n'est trié c'est immédiat.

— Supposons que le tableau soit trié jusqu'au ie chiffre. Alors au $i+1$e tour de boucle on trie de manière stable selon le $i+1$e chiffre. Soit x, y deux éléments de A tronqués au $i+1$e chiffre, et soit $x = x_{i+1}x_i \dots x_1$ et $y = y_{i+1}y_i \dots y_1$ leur écriture en base k. Supposons que $x > y$.

  — Si $x_{i+1} > y_{i+1}$ alors x est placé après y par le tri par le $i+1$e chiffre.

  — Si $x_{i+1} = y_{i+1}$ alors $x_i \dots x_1 > y_i \dots y_1$, et donc par le tri précédent, x est placé après y. Puisque le tri par dénombrement est stable, x est encore placé après y dans le tri en cours.

  Ainsi le tableau est trié jusqu'au $i+1$e chiffre après le tri du $i+1$e chiffre.

À la fin de l'algorithme, le tableau est donc trié. □

Complexité tri par base. Le tri par base procède à d tris par dénombrement de paramètres A, k. Donc chaque tour de boucle nécessite $O(n+k)$ opérations. D'où un coût en $O(d(n+k))$. □

Troisième partie

Lecons

CHAPITRE 6

ALGÈBRE

101 Groupe opérant sur un ensemble. Exemples et applications

101.1 Développements

— 12 - Isométries du cube et représentations de $\mathfrak{S}_4$.

— 25 - Réciprocité quadratique par les formes quadratiques.

101.2 Rapport de Jury

Dans cette leçon, il faut bien dominer les deux approches de l'action de groupe : l'approche naturelle et l'approche via le morphisme du groupe agissant vers le groupe des permutations de l'ensemble sur lequel il agit. La formule des classes et ses applications immédiates sont incontournables. Des exemples de natures différentes doivent être présentés : actions sur un ensemble fini, sur un espace vectoriel (en particulier les représentations), sur un ensemble de matrices, sur des groupes ou des anneaux. Les exemples issus de la géométrie ne manquent pas (groupes d'isométries d'un solide ou d'un polygone régulier). Il est important de savoir calculer des stabilisateurs et des orbites notamment dans le cadre de l'action par conjugaison. Les théorèmes de Sylow peuvent avoir leur place dans cette leçon.

Parmi les applications des actions de groupes, on pourra citer des résultats de dénombrement, comme par exemple la formule de Lucas qui permet de calculer efficacement les cœfficients binomiaux.

S'ils le désirent, les candidats peuvent aller plus loin en décrivant les actions naturelles de $PGL(2, \mathbb{F}_q)$ sur la droite projective, ou de $SL_2(Z)$ sur le demi-plan de Poincaré.

En notant que l'injection du groupe de permutations dans le groupe linéaire par les matrices de permutations donne lieu à des représentations, ils pourront facilement en déterminer le caractère.

104 Groupes finis. Exemples et applications

104.1 Développements

— 12 - Isométries du cube et représentations de $\mathfrak{S}_4$.

— 29 - Théorème de structure des groupes abéliens finis.

104.2 Rapport de Jury

Dans cette leçon il faut savoir manipuler correctement les éléments de différentes structures usuelles ($\mathbb{Z}/n\mathbb{Z}$, $\mathfrak{S}_n$, etc.) comme, par exemple, en proposer un générateur ou une famille de générateurs, savoir calculer un produit de deux permutations, savoir décomposer une permutation en produit de cycles à supports disjoints. Il est important que la notion d'ordre d'un élément soit mentionnée et comprise dans des cas simples. Le théorème de structure des groupes abéliens finis doit être connu. Il est bon de connaître les groupes d'ordre p et p^2 pour p premier ainsi que les groupes d'ordre inférieur à 8.

Les exemples doivent figurer en bonne place dans cette leçon. Les groupes d'automorphismes fournissent des exemples très naturels. On peut aussi étudier les groupes de symétries $\mathfrak{A}_4$, $\mathfrak{S}_4$, $\mathfrak{A}_5$ et relier sur ces exemples géométrie et algèbre, les représentations ayant ici toute leur place ; il est utile de connaître les groupes diédraux.

S'ils le désirent, les candidats peuvent ensuite mettre en avant les spécificités de groupes comme le groupe quaternionique, les sous-groupes finis de $SU(2)$ ou les groupes $GL_n(\mathbb{F}_q)$.

105 Groupes de permutations d'un ensemble fini. Applications

105.1 Développements

— 12 - Isométries du cube et représentations de $\mathfrak{S}_4$.

— 09 - Théorème de Frobenius-Zolotarev.

105.2 Rapport de Jury

Parmi les attendus, il faut savoir relier la leçon avec les notions d'orbites et d'actions de groupes. Il faut aussi savoir décomposer une permutation en cycles à supports disjoints, tant sur le plan théorique (preuve du théorème de décomposition), que pratique (sur un exemple). Il est important de savoir déterminer les classes de conjugaisons du groupe symétrique par la décomposition en cycles, d'être capable de donner des systèmes de générateurs.

L'existence du morphisme signature est un résultat non trivial mais ne peut pas constituer, à elle seule, l'objet d'un développement. Il est bon d'avoir en tête que tout groupe fini se plonge dans un groupe symétrique et de savoir calculer la signature des permutations ainsi obtenues dans des cas concrets. Les applications sont nombreuses, il est très naturel de parler du déterminant, des polynômes symétriques ou des fonctions symétriques des racines d'un polynôme. On peut également parler du lien avec les groupes d'isométries des solides.

S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant aux automorphismes du groupe symétrique, à des problèmes de dénombrement, aux représentations des groupes des permutations ou encore aux permutations aléatoires.

106 Groupe linéaire d'un espace vectoriel de dimension finie E, sous-groupes de GL(E). Applications.

106.1 Développements :

— 17 - Théorème de Lie-Kolchin.

— 14 - Sous groupes compacts de $GL_n(\mathbb{R})$.

106.2 Rapport de Jury

Cette leçon ne doit pas se résumer à un catalogue de résultats épars sur $GL(E)$. Il est important de savoir faire correspondre les sous-groupes du groupe linéaire avec les stabilisateurs de certaines actions naturelles (sur des formes quadratiques, symplectiques, sur des drapeaux, sur une décomposition en somme directe, etc.). On doit présenter des systèmes de générateurs de $GL(E)$ et étudier la topologie de ce groupe en précisant pourquoi le choix du corps de base est important. Les liens avec le pivot de Gauss sont à détailler. Il faut aussi savoir réaliser $\mathfrak{S}_n$ dans $GL(n, K)$ et faire le lien entre signature et déterminant, et entre les classes de conjugaison et les classes de similitude.

S'ils le désirent, les candidats peuvent aller plus loin en remarquant que la théorie des représentations permet d'illustrer l'importance de $GL_n(C)$ et de son sous-groupe unitaire.

108 Exemples de parties génératrices d'un groupe. Applications

108.1 Développements :

— 24 - $SO(3)$ et les quaternions.

— 09 - Groupe dérivé de $GL(n)$ et application à Frobenius-Zolotarev.

108.2 Rapport de Jury

C'est une leçon qui doit être illustrée par des exemples très variés qui peuvent être en relation avec les groupes de permutations, les groupes linéaires ou leurs sous-groupes, comme $SL_n(K)$, $O_n(R)$ ou $SO_n(R)$. Les groupes $\mathbb{Z}/n\mathbb{Z}$, fournissent aussi des exemples intéressants. La connaissance de parties génératrices s'avère très utile dans l'analyse des morphismes de groupes ou pour montrer la connexité par arcs de certains sous-groupes de $Gl_n(R)$ par exemple.

Tout comme dans la leçon 106, la présentation du pivot de Gauss et de ses applications est envisageable.

Il est important de présenter les différents systèmes de générateurs du groupe symétrique et de savoir mettre en évidence l'intérêt du choix de ces systèmes dans divers exemples.

Le candidat pourra également parler des générateurs du groupe diédral et, si il le souhaite, il pourra donner une présentation par générateurs et relations d'un groupe (groupe diédral, groupe symétrique, ou groupe des tresses).

Il est également possible de parler du logarithme discret et de ses applications à la cryptographie (algorithme de Diffie-Hellman, cryptosystème de El Gamal)

120 Anneaux $\mathbb{Z}/n\mathbb{Z}$. Applications

120.1 Développements :

— 29 - Théorème de structure des groupes abéliens finis.

— 18 - Primalité des nombres de Mersenne.

120.2 Rapport de Jury

Dans cette leçon, l'entier n n'est pas forcément un nombre premier. Il est utile de connaître et d'étudier le groupe des inversibles de l'anneau et les idéaux de $\mathbb{Z}/n\mathbb{Z}$.

Il est nécessaire de bien maîtriser le théorème chinois et sa réciproque. S'ils le désirent, les candidats peuvent poursuivre en donnant une généralisation du théorème chinois lorsque deux éléments ne sont pas premiers entre eux, ceci en faisant apparaître le PGCD et le PPCM de ces éléments.

Il faut bien sûr savoir appliquer le théorème chinois à l'étude du groupe des inversibles et, ainsi, retrouver la multiplicativité de l'indicatrice d'Euler. Toujours dans le cadre du théorème chinois, il est bon de distinguer clairement les propriétés de groupes additifs et d'anneaux.

Enfin, il est indispensable de présenter quelques applications arithmétiques des propriétés des anneaux $\mathbb{Z}/n\mathbb{Z}$, telles que l'étude de quelques équations diophantiennes bien choisies. De même, les applications cryptographiques telles que l'algorithme RSA sont naturelles dans cette leçon.

S'ils le désirent, les candidats peuvent aller plus loin en s'intéressant au calcul effectif des racines carrées dans $\mathbb{Z}/n\mathbb{Z}$, au logarithme discret, ou à la transformée de Fourier rapide. Il est également possible de parler des nombres p-adiques.

121 Nombres premiers. Applications

121.1 Développements :

— 28 - Théorème de Sophie Germain.

— 18 - Primalité des nombres de Mersenne.

121.2 Rapport de Jury

Le sujet de cette leçon est très vaste. Aussi les choix devront être clairement motivés. La réduction modulo p n'est pas hors-sujet et constitue un outil puissant pour résoudre des problèmes arithmétiques simples. La répartition des nombres premiers est un résultat historique important qu'il faudrait citer. Sa démonstration n'est bien sûr pas exigible au niveau de l'agrégation.

Quelques résultats sur les corps finis et leur géométrie sont les bienvenus, ainsi que des applications en cryptographie.

123 Corps finis. Applications.

123.1 Développements :

— 02 - Algorithme de Berlekamp.

— 25 - Théorème de la réciprocité quadratique.

123.2 Rapport de Jury

Une construction des corps finis doit être connue et une bonne maîtrise des calculs dans les corps finis est indispensable. Les injections des divers $\mathbb{F}_q$ doivent être connues. Les applications des corps finis (y compris pour $\mathbb{F}_q$ avec q non premier !) ne doivent pas être oubliées, par exemple l'étude de polynômes à coefficients entiers et de leur irréductibilité peut figurer dans cette leçon. Le calcul des degrés des extensions et le théorème de la base téléscopique sont incontournables. La structure du groupe multiplicatif doit aussi être connue. L'étude des carrés dans un corps fini et la résolution d'équations de degré 2 sont envisageables.

S'ils le désirent, les candidats peuvent aller plus loin en détaillant des codes correcteurs ou en étudiant l'irréductiblilité des polynômes à coefficients dans un corps fini.

126 Exemples d'équations en arithmétique

126.1 Développements :

— 28 - Théorème de Sophie Germain.

— 25 - Loi de la réciprocité quadratique.

126.2 Rapport de Jury

Pour la session 2019, le titre de cette leçon évolue en

Exemples d'équations en arithmétique.

[Cette leçon était auparavant intitulée

Exemples d'équations diophantiennes].

Ce nouvel intitulé traduit le souhait d'élargir le contexte de la leçon, au delà des seules équations sur $\mathbb{Z}$ pour étudier aussi des équations dans $\mathbb{Z}/n\mathbb{Z}$ et dans les corps finis.

Malgré le changement d'intitulé, les équations diophantiennes occupent une place importante et doivent absolument être abordées dans cette leçon. On doit présenter les notions de bases servant à aborder les équations de type $ax + by = d$ (identité de Bezout, lemme de Gauss) mais aussi bien entendu la méthode de descente de Fermat et l'utilisation de la réduction modulo un nombre premier p. La leçon peut aussi dériver vers la notion de factorialité, illustrée par des équations de type Mordell, Pell-Fermat, et même Fermat (pour $n = 2$, ou pour les nombres premiers de Sophie Germain). La résolution des systèmes linéaires sur $\mathbb{Z}$ peut être abordée.

Il est naturel de s'intéresser à la résolution des systèmes de congruences, à la recherche de racines carrées dans les corps finis. Les candidats peuvent plus généralement aborder la recherche des racines des polynômes dans les corps finis.

S'il le désirent, les candidats peuvent étudier les coniques sur les corps finis et la recherche de points sur ces coniques.

126.3 Plan

On suit les recommandations du jury en ne se contentant pas que des équations dans $\mathbb{Z}$. Ça tombe bien, c'est plus amusant (je trouve) de parler d'équations dans les corps finis.

On fait un plan thématique. On introduit les équations à coefficients entier de la forme $ax + by = d$ comme le propose le Jury, et on donne des exemples. Ensuite, on parle longuement de Fermat parce que ça a un intérêt historique, parce que c'est pédagogique, et parce que c'est notre premier développement. On présente le principe de descente infini de Fermat et les méthodes de résolutions pour $n = 3, 4$ [Hin00]. On n'oublie pas d'énoncer le théorème général, ça serait dommage !

On présente ensuite le théorème des 2 et 4 carrés, en passant dans $\mathbb{Z}[i]$ et les quaternions. On peut brièvement évoquer Dirichlet pour dire qu'il y a une infinité d'équations avec des solutions.

Puis on parle de réduction modulo p. C'est l'occasion de faire un apparté sur les corps finis et leurs équations. On donne des exemples, on propose les liens avec les extensions de corps finis. Mais on se focalise surtout sur les équations de degré 2. On donne la méthode

générale, ce qui permet de motiver le calcul des carrés et on balance la loi de réciprocité quadratique (Deuxième développement) et Chevalley Warning ([CG13] et [CG17a]).

Enfin, on peut conclure en citant le 10*eme* problème de Hilbert, et les liens avec la décidabilité. Mais c'est une ouverture, et j'ai pas de ref.

141 Polynômes irréductibles à une indéterminée. Corps de rupture. Exemples et applications

141.1 Développements :

— 02 - Algorithme de Berlekamp.

— 18 - Primalité des nombres de Mersenne.

141.2 Rapport de Jury

La présentation du bagage théorique permettant de définir corps de rupture, corps de décomposition, ainsi que des illustrations dans différents types de corps (réel, rationnel, corps finis) sont inévitables. Les corps finis peuvent être illustrés par des exemples de polynômes irréductibles de degré 2, 3, 4 sur $\mathbb{F}_2$ ou $\mathbb{F}_3$. Il est nécessaire de présenter des critères d'irréductibilité de polynômes et des polynômes minimaux de quelques nombres algébriques.

Il faut savoir qu'il existe des corps algébriquement clos de caractéristique nulle autres que $\mathbb{C}$; il est bon de savoir montrer que l'ensemble des nombres algébriques sur le corps $\mathbb{Q}$ des rationnels est un corps algébriquement clos. Le théorème de la base téléscopique, ainsi que les utilisations arithmétiques (utilisation de la divisibilité) que l'on peut en faire dans l'étude de l'irréductibilité des polynômes, est incontournable.

151 Dimension d'un espace vectoriel (on se limitera au cas de la dimension finie). Rang. Exemples et applications

151.1 Développements :

— 33 - Théorème des sous-variétés et application au théorème des extrema liés.

— 10 - Théorème des invariants de Similitude.

151.2 Rapport de Jury

Dans cette leçon, il est indispensable de présenter les résultats fondateurs de la théorie des espaces vectoriels de dimension finie en ayant une idée de leurs preuves. Ces théorèmes semblent simples car ils ont été très souvent pratiqués, mais leur preuve demande un soin particulier. Il est important de savoir justifier pourquoi un sous-espace vectoriel d'un espace vectoriel de dimension finie est aussi dedimension finie. Le pivot de Gauss ainsi que les diverses notions et caractérisations du rang trouvent leur place dans cette leçon. Les applications sont nombreuses, on peut par exemple évoquer l'existence de polynômes annulateurs ou alors décomposer les isométries en produits de réflexions.

On pourra utiliser les caractérisations du rang pour démontrer l'invariance du rang par extension de corps, ou pour établir des propriétés topologiques (sur $\mathbb{R}$ ou $\mathbb{C}$).

S'ils le désirent, les candidats peuvent déterminer des degrés d'extensions dans la théorie des corps ou s'intéresser aux nombres algébriques.

On pourra également explorer des applications en analyse comme les extrémas liés ou l'étude de l'espace vectoriel engendré par les translatés d'une application de $\mathbb{R}$ dans $\mathbb{R}$.

Dans un autre registre, il est pertinent d'évoquer la méthode des moindres carrés dans cette leçon, par exemple en faisant ressortir la condition de rang maximal pour garantir l'unicité de la solution et s'orienter vers les techniques de décomposition en valeurs singulières pour le cas général. On peut alors naturellement explorer l'approximation d'une matrice par une suite de matrices de faible rang.

152 Déterminant. Exemples et applications.

152.1 Développements :

— 30 - Suite de Polygones.

— 09 - Théorème de Frobenius Zolotarev.

152.2 Rapport de Jury

Dans cette leçon, il faut commencer par définir correctement le déterminant. Il est possible d'entamer la leçon en disant que le sous-espace des formes n-linéaires alternées sur un espace de dimension n est de dimension 1 et, dans ce cas, il est essentiel de savoir le montrer. Le plan doit être cohérent ; si le déterminant n'est défini que sur $\mathbb{R}$ ou $\mathbb{C}$, il est délicat de définir $\det(A-XI_n)$ avec A une matrice carrée. L'interprétation du déterminant comme volume est essentielle. On peut rappeler son rôle dans les formules de changement de variables, par exemple pour des transformations de variables aléatoires.

Le calcul explicite est important, mais le jury ne peut se contenter d'un déterminant de Vandermonde ou d'un déterminant circulant. Les opérations élémentaires permettant de calculer des déterminants, avec des illustrations sur des exemples, doivent être présentées. Il est bienvenu d'illustrer la continuité du déterminant par une application, ainsi que son caractère polynomial. Pour les utilisations des propriétés topologiques, on n'omettra pas de préciser le corps de base sur lequel on se place.

S'ils le désirent, les candidats peuvent s'intéresser aux calculs de déterminants sur $\mathbb{Z}$ avec des méthodes multimodulaires. Le résultant et les applications simples à l'intersection ensembliste de deux courbes algébriques planes peuvent aussi trouver leur place dans cette leçon pour des candidats ayant une pratique de ces notions.

153 Polynômes d'endomorphisme en dimension finie. Réduction d'un endomorphisme en dimension finie. Applications.

153.1 Développements :

— 10 - Invariants de similitudes.

— 07 - Un algorithme pour la décomposition de Dunford.

153.2 Rapport de Jury

Cette leçon ne doit pas être un catalogue de résultats autour de la réduction qui est ici un moyen pour démontrer des théorèmes ; les polynômes d'endomorphismes doivent y occuper une place importante. Il faut consacrer une courte partie de la leçon à l'algèbre $K[u]$ et connaître sa dimension sans hésitation. Il est ensuite possible de s'intéresser aux propriétés globales de cette algèbre.

Les liens entre réduction d'un endomorphisme u et la structure de l'algèbre $K[u]$ sont importants, tout comme ceux entre les idempotents et la décomposition en somme de sous-espaces caractéristiques. Il faut bien préciser que, dans la réduction de Dunford, les composantes sont des polynômes en l'endomorphisme, et en connaître les conséquences théoriques et pratiques.

L'aspect *applications* est trop souvent négligé. Il est possible, par exemple, de mener l'analyse spectrale de matrices stochastiques. On attend d'un candidat qu'il soit en mesure, pour une matrice simple de justifier la diagonalisabilité et de déterminer un polynôme annulateur (voire minimal). Il est bien sûr important de ne pas faire de confusion entre diverses notions de multiplicité pour une valeur propre λ donnée (algébrique ou géométrique). Enfin, calculer A^k ne nécessite pas, en général, de réduire A (la donnée d'un polynôme annulateur de A suffit souvent). Il est possible d'envisager des applications aux calculs d'exponentielles de matrices.

S'il le souhaite, le candidat pourra étudier des équations matricielles et de calcul fonctionnel, avec par exemple l'étude de l'extraction de racines ou du logarithme.

156 Exponentielle de matrices. Applications

156.1 Développements

— 04 - Théorème de Cartan Von Neumann.

— 06 - Etude du groupe $O(p, q)$.

156.2 Rapport du Jury

Bien que ce ne soit pas une leçon d'analyse, il faut toutefois pouvoir justifier clairement la convergence de la série exponentielle. La distinction entre le cas réel et complexe doit être clairement évoqué.

Les questions de surjectivité ou d'injectivité doivent être abordées. Par exemple la matrice

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

est-elle l'exponentielle d'une matrice à coefficients réels ? La matrice définie par blocs

$$B = \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

est-elle l'exponentielle d'une matrice à coefficients réels ?

La décomposition de Dunford multiplicative (décomposition de Jordan) de $exp(A)$ trouve toute son utilité dans cette leçon. Notons que l'exponentielle fait bon ménage avec la décomposition polaire dans bon nombre de problèmes sur les sous-groupes du groupe linéaire. L'étude du logarithme (quand il est défini) trouve toute sa place dans cette leçon. Si l'on traite du cas des matrices nilpotentes, on pourra évoquer le calcul sur les développements limités.

Il est bon de connaître l'image par exponentielle de certains sous-ensembles de matrices (ensemble des matrices symétriques, hermitiennes, ou antisymétriques).

Les applications aux équations différentielles méritent d'être présentées sans toutefois constituer l"essentiel de la leçon. On pourra par exemple faire le lien entre réduction et comportement asymptotique, mais le jury déconseille aux candidats de proposer ce thème dans un développement de cette leçon, sauf à avoir bien compris comment les apports algébriques permettent ici de simplifier les conclusions analytiques.

S'ils le désirent, les candidats peuvent s'aventurer vers les sous-groupes à un paramètre du groupe linéaire (on peut alors voir si ces sous-groupes constituent des sous-variétés fermées de $GL(n, R)$) ou vers les algèbres de Lie.

157 Endomorphismes trigonalisables. Endomorphismes nilpotents.

157.1 Développements

— 17 - Théorème de Lie-Kolchin.

— 07 - Un algorithme pour la décomposition de Dunford.

157.2 Rapport du Jury

Il est bon de savoir expliquer pourquoi l'application induite par un endomorphisme trigonalisable (respectivement nilpotent) sur un sous-espace stable est encore trigonalisable (respectivement nilpotent). L'utilisation des noyaux itérés est fondamentale dans cette leçon, par exemple pour déterminer si deux matrices nilpotentes sont semblables. Il est intéressant de présenter des conditions suffisantes de trigonalisation simultanée ; l'étude des endomorphismes cycliques a toute sa place dans cette leçon. L'étude des nilpotents en dimension 2 débouche naturellement sur des problèmes de quadriques et l'étude sur un corps fini donne lieu à de jolis problèmes de dénombrement.

S'ils le désirent, les candidats peuvent aussi présenter la décomposition de Frobenius, ou des caractérisations topologiques des endomorphismes nilpotents, ou encore des propriétés topologiques de l'ensemble des endomorphismes nilpotents.

159 Formes linéaires et dualité en dimension finie. Exemples et applications.xs

159.1 Développements

— 10 - Invariants de similitude et décomposition de Frobenius.

— 33 - Théorème des extrema liés.

159.2 Rapport du Jury

Il est important de bien placer la thématique de la dualité dans cette leçon ; celle-ci permet de mettre en évidence des correspondances entre un morphisme et son morphisme transposé, entre un sous-espace et son orthogonal (canonique), entre les noyaux et les images ou entre les sommes et les intersections. Bon nombre de résultats d'algèbre linéaire se voient dédoublés par cette correspondance. Les liens entre base duale et fonctions de coordonnées doivent être parfaitement connus. Le passage d'une base à sa base duale ou antédualte, ainsi que les formules de changement de base, doivent être maîtrisés. On pourra s'intéresser aux cas spécifiques où l'isomorphisme entre l'espace et son dual est canonique (cas euclidien, cas des matrices).

Savoir calculer la dimension d'une intersection d'hyperplans via la dualité est important dans cette leçon. L'utilisation des opérations élémentaires sur les lignes et les colonnes permet facilement d'obtenir les équations d'un sous-espace vectoriel ou d'exhiber une base d'une intersection d'hyperplans.

Cette leçon peut être traitée sous différents aspects : géométrique, algébrique, topologique ou analytique. Il faut que les développements proposés soient en lien direct avec la leçon. Enfin rappeler que la différentielle d'une fonction à valeurs réelles est une forme linéaire semble incontournable.

Il est possible d'illustrer la leçon avec un point de vue probabiliste, en rappelant que la loi d'un vecteur aléatoire X est déterminée par les lois unidimensionnelles de $X \cdot u$ pour tout vecteur u.

162 Systèmes d'équations linéaires ; opérations élémentaires, aspects algorithmiques et conséquences théoriques.

162.1 Développements

— 19 - Méthode itérative de résolution d'un système linéaire.

— 09 - Groupe dérivé de $GL(n)$ et théorème de Frobenius Zolotarev.

— 02 - Algorithme de Berlekamp.

162.2 Rapport du Jury

Dans cette leçon, les techniques liées au simple pivot de Gauss constituent l'essentiel des attendus. Il est impératif de faire le lien avec la notion de système échelonné, (dont on donnera une définition précise et correcte), et de situer l'ensemble dans le contexte de l'algèbre linéaire (sans oublier la dualité). Un point de vue opératoire doit accompagner l'étude théorique et l'intérêt algorithmique des méthodes présentées doit être expliqué. On pourra illustrer cela par des exemples simples (où l'on attend parfois une résolution explicite).

Parmi les conséquence théoriques, les candidats pourront notamment donner des systèmes de générateurs de $(GL_n(K)$ et $SL_n(K)$. Ils peuvent aussi présenter les relations de dépendance linéaire sur les colonnes d'une matrice échelonnée qui permettent de décrire simplement les orbites de l'action à gauche de $GL(n, K)$ sur $M_n(K)$ donnée par $(P, A) \mapsto PA$.

S'ils le désirent, les candidats peuvent exploiter les propriétés des systèmes d'équations linéaires pour définir la dimension des espaces vectoriels et obtenir une description de l'intersection de deux sous espaces vectoriels donnés par des systèmes générateurs, ou d'une somme de deux sous-espaces vectoriels donnés par des équations.

De même, des discussions sur la résolution de systèmes sur $\mathbb{Z}$ et la forme normale de Hermite peuvent trouver leur place dans cette leçon. Enfin, il est possible de présenter les décompostions LU et de Choleski, en évaluant le coût de ces méthodes ou encore d'étudier la résolution de l'équation normale associée aux problèmes des moindres carrés et la détermination de la solution de norme minimale par la méthode de décomposition en valeurs singulières.

170 Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

170.1 Développements

— 06 - Etude du groupe d'isométrie d'une forme quadratique réelle.

— 25 - Loi de la réciprocité quadratique.

170.2 Rapport du Jury

Il faut tout d'abord noter que l'intitulé implique implicitement que le candidat ne doit pas se contenter de travailler sur $\mathbb{R}$. Le candidat pourra parler de la classification des formes quadratiques sur le corps des complexes et sur les corps finis. L'algorithme de Gauss doit être énoncé et pouvoir être mis en œuvre sur une forme quadratique simple.

Les notions d'isotropie et de cône isotrope sont un aspect important de cette leçon. On pourra rattacher cette notion à la géométrie différentielle.

182 Applications des nombres complexes à la géométrie

182.1 Développements

— 30 - Convergence d'une suite de polygones.

— 24 - $SO(3)$ et les quaternions.

182.2 Rapport du Jury

Cette leçon ne doit pas rester au niveau de la classe de Terminale. L'étude des inversions est tout à fait appropriée, en particulier la possibilité de ramener un cercle à une droite et inversement ; la formule de Ptolémée illustre bien l'utilisation de cet outil. On peut parler des suites définies par récurrence par une homographie et leur lien avec la réduction dans $SL_n(C)$.

S'ils le désirent, les candidats peuvent aussi étudier l'exponentielle complexe et les homographies de la sphère de Riemann. La réalisation du groupe SU_2 dans le corps des quaternions et ses applications peuvent trouver leur place dans la leçon. Il est possible de présenter les similitudes, les homographies et le birapport.

183 Utilisation des groupes en géométrie

183.1 Développements

— 12 - Groupe d'isométries du cube et représentations de $\mathfrak{S}_4$.

— 24 - $SO(3)$ et les quaternions.

183.2 Rapport du Jury

C'est une leçon dans laquelle on s'attend à trouver des utilisations variées. On s'attend à ce que soient définis différents groupes de transformations (isométries, déplacements, similitudes, translations) et à voir résolus des problèmes géométriques par des méthodes consistant à composer des transformations. De plus, les actions de groupes sur la géométrie permettent aussi de dégager des invariants essentiels (angle, birapport, excentricité d'une conique). Les groupes d'isométries d'une figure sont incontournables.

183.3 Plan

Première partie : Définitions, introductions
On commence par définir le groupe affine et sa structure dans une première partie. x

Deuxième partie : Utilisation des groupes pour de la classification
Ensuite, on montre comment les groupes peuvent servir, par leur action, à classifier des éléments géométriques, et on donne l'exemple de la classification des coniques par l'action de $GL_2(\mathbb{R})$ sur $\mathcal{S}_2(\mathbb{R})$.

Troisième partie : Groupes des isométries conservant une partie On parle d'abord des groupes d'isométries de polygônes réguliers dans le plan avec les groupes diedraux. C'est l'occasion d'aborder les représentations du groupe symétrique : On commence par la représentation de $\mathfrak{S}_3$ de degré 2 et on donne sa table de caractères. Puis on parle des isométries conservant une partie de $\mathbb{R}^3$. On balance notre premier développement sur les isométries du cube et on dresse la table de caractères de $\mathfrak{S}_4$.

Quatrième partie : On parle des quaternions On reste dans $\mathbb{R}^3$ et on aborde la paramétrisation des rotations via les quaternions, ce qui fait l'objet du second développement.

190 Méthodes combinatoires, problèmes de dénombrement

190.1 Développements

— 25 - Loi de la réciprocité quadratique par double dénombrement.

— 01 - Dénombrement des partitions d'un ensemble fini, via les séries entières.

190.2 Rapport du Jury

Il est nécessaire de dégager clairement différentes méthodes de dénombrement et de les illustrer d'exemples significatifs. De nombreux domaines de mathématiques sont concernés par des problèmes de dénombrement, cet aspect varié du thème de la leçon doit être mis en avant. L'utilisation de séries génératrices est un outil puissant pour le calcul de certains cardinaux. De plus, il est naturel de calculer des cardinaux classiques et certaines probabilités. Il est important de connaître l'interprétation ensembliste de la somme des coefficients binomiaux et ne pas se contenter d'une justification par le binôme de Newton. L'introduction des corps finis (même en se limitant aux cardinaux premiers) permet de créer un lien avec l'algèbre linéaire. Les actions de groupes peuvent également conduire à des résultats remarquables.

S'ils le désirent, les candidats peuvent aussi présenter des applications de la formule d'inversion de Möebius ou de la formule de Burnside. Des candidats ayant un bagage probabiliste pourront explorer le champ des permutations aléatoires, en présentant des algorithmes pour générer la loi uniforme sur le groupe symétrique Sn et analyser certaines propriétés de cette loi uniforme (points fixes, cycles, limite $n \to +\infty$ ...).

CHAPITRE 7

ANALYSE

203 Utilisation de la notion de compacité.

203.1 Développements

— 08 - Opérateurs compacts et alternative de Fredholm.

— 14 - Sous-groupes compacts de $GL_n(\mathbb{R})$.

203.2 Rapport du Jury

Il est important de ne pas concentrer la leçon sur la compacité en général et d'éviter la confusion entre utilisation de la notion compacité et notion de compacité. Le jury recommande vivement de rester en priorité dans le cadre métrique. Néanmoins, on attend des candidats d'avoir une vision synthétique de la compacité. Des exemples d'applications comme le théorème de Heine et le théorème de Rolle doivent y figurer et leur démonstration être connue. Par ailleurs, le candidat doit savoir quand la boule unité d'un espace vectoriel normé est compacte. Des exemples significatifs d'utilisation comme le théorème de Stone-Weierstrass (version qui utilise la compacité), des théorèmes de point fixe, voire l'étude qualitative d'équations différentielles, sont tout à fait envisageables. Le rôle de la compacité pour des problèmes d'existence d'extrema mériterait d'être davantage étudié. On peut penser ensuite à des exemples en dimension $n \geq 2$.

Pour aller plus loin, les familles normales de fonctions holomorphes fournissent des exemples fondamentaux d'utilisation de la compacité. Les opérateurs auto-adjoints compacts sur un espace de Hilbert relèvent également de cette leçon, et on pourra développer l'analyse de leurs propriétés spectrales.

208 Espaces vectoriels normés, applications linéaires continues. Exemples.

208.1 Développements

— 08 - Opérateurs compacts et alternative de Fredholm.

— 14 - Sous-groupes compacts de $GL_n(\mathbb{R})$.

— 27 - Résolution d'une équation différentielle via $H_0^1(0,1)$.

208.2 Rapport du Jury

Le jury rappelle qu'une telle leçon doit contenir beaucoup d'illustrations et d'exemples, notamment avec quelques calculs élémentaires de normes subordonnées (notion qui met en difficulté un trop grand nombre de candidats). Le lien avec la convergence des suites du type $X_{n+1} = AX_n$ doit être connu (et éventuellement illustré, sans que cela puisse être mis au cœur de la leçon, de considérations d'analyse numérique matricielle). Lors du choix de ces exemples, le candidat veillera à ne pas mentionner des exemples pour lesquels il n'a aucune idée de leur pertinence et à ne pas se lancer dans des développements trop sophistiqués.

La justification de la compacité de la boule unité en dimension finie doit être maîtrisée. Il faut savoir énoncer le théorème de Riesz sur la compacité de la boule unité fermée d'un espace vectoriel normé. Le théorème d'équivalence des normes en dimension finie, ou le caractère fermé de tout sous-espace de dimension finie d'un espace normé, sont des résultats fondamentaux à propos desquels les candidats doivent se garder des cercles vicieux. Des exemples d'espaces vectoriels normés de dimension infinie ont leur place dans cette leçon et il faut connaître quelques exemples de normes usuelles non équivalentes, notamment sur des espaces de suites ou des espaces de fonctions et également d'applications linéaires qui ne sont pas continues. On peut aussi illustrer le théorème de Riesz sur des exemples simples dans le cas des espaces classiques de dimension infinie.

Les espaces de Hilbert ont également leur place dans cette leçon, mais le jury met en garde contre l'écueil de trop s'éloigner du cœur du sujet.

214 Théorème d'inversion locale, théorème des fonctions implicites. Exemples et applications en analyse et en géométrie.

214.1 Développements

— 33 - Théorème des sous-variétés, et extrema liés.

— 04 - Théorème de Cartan Von Neumann.

214.2 Rapport du Jury

Il s'agit d'une leçon qui exige une bonne maîtrise du calcul différentiel. Même si le candidat ne propose pas ces thèmes en développement, on est en droit d'attendre de lui des idées de démonstration des deux théorèmes fondamentaux qui donnent son intitulé à la leçon. Il est indispensable de savoir mettre en pratique le théorème des fonctions implicites au moins dans le cas de deux variables réelles. On attend des applications en géométrie différentielle notamment dans la formalisation de la méthode des multiplicateurs de Lagrange. En ce qui concerne la preuve du théorème des extrema liés, la présentation de la preuve par raisonnement « sous-matriciel » est souvent obscure ; on privilégiera si possible une présentation géométrique s'appuyant sur l'espace tangent. Plusieurs inégalités classiques de l'analyse peuvent se démontrer avec ce point de vue : arithmético-géométrique, Hölder, Carleman, Hadamard,... Pour aller plus loin, l'introduction des sous-variétés est naturelle dans cette leçon. Il s'agit aussi d'agrémenter cette leçon d'exemples et d'applications en géométrie, sur les courbes et les surfaces.

219 Extremums : existence, caractérisation, recherche. Exemples et applications.

219.1 Développements

— 33 - Théorème des sous-variétés, et extrema liés.

— 20 - Optimisation convexe dans un Hilbert.

219.2 Rapport du Jury

Comme souvent en analyse, il est tout à fait opportun d'illustrer dans cette leçon un exemple ou un raisonnement à l'aide d'un dessin. Il faut savoir faire la distinction entre propriétés locales (caractérisation d'un extremum local) et globales (existence par compacité, par exemple). Dans le cas important des fonctions convexes, un minimum local est également global. Les applications de la minimisation des fonctions convexes sont nombreuses et elles peuvent illustrer cette leçon.

L'étude des algorithmes de recherche d'extremums y a toute sa place : méthode du gradient et analyse de sa convergence, méthode à pas optimal,... Le cas particulier des fonctionnelles sur $\mathbb{R}^n$ de la forme $\frac{1}{2}\langle Ax|x\rangle + \langle b|x\rangle$, où A est une matrice symétrique définie positive, ne devrait pas poser de difficultés (la coercivité de la fonctionnelle pose problème à de nombreux candidats). Les problèmes de minimisation sous contrainte amènent à faire le lien avec les extrema liés et la notion de multiplicateur de Lagrange. Sur ce point, certains candidats ne font malheureusement pas la différence entre recherche d'extremums sur un ouvert ou sur un fermé. Une preuve géométrique des extrema liés sera fortement valorisée par rapport à une preuve algébrique, formelle et souvent mal maîtrisée. On peut ensuite mettre en œuvre ce théorème en justifiant une inégalité classique : arithmético-géométrique, Hölder, Carleman, etc... Enfin, la question de la résolution de l'équation d'Euler-Lagrange peut donner l'opportunité de mentionner la méthode de Newton.

Les candidats pourraient aussi être amenés à évoquer les problèmes de type moindres carrés, ou, dans un autre registre, le principe du maximum et des applications.

220 Équations différentielles $X' = f(t, X)$. Exemples d'études des solutions en dimension 1 et 2

220.1 Développements

— 16 - Stabilité d'un système différentiel autonome.

— 27 - Étude d'une équation différentielle d'ordre 2 avec conditions au bord.

220.2 Rapport du Jury

Une nouvelle fois, le jury s'alarme des nombreux défauts de maîtrise du théorème de Cauchy-Lipschitz et, plus généralement, de l'extrême faiblesse des connaissances sur les équations différentielles. Il est regrettable de voir des candidats ne connaître qu'un énoncé pour les fonctions globalement lipschitziennes ou, plus grave, mélanger les conditions sur la variable de temps et d'état. Les notions de solution maximale et de solution globale sont souvent confuses. Le théorème de sortie de tout compact est attendu. Bien évidemment, le jury attend des exemples d'équations différentielles non linéaires. Le lemme de Grönwall semble trouver toute sa place dans cette leçon mais est trop rarement énoncé. L'utilisation du théorème de Cauchy-Lipschitz doit pouvoir être mise en œuvre sur des exemples concrets. Les études qualitatives doivent être préparées et soignées.

Pour les équations autonomes, la notion de point d'équilibre permet des illustrations pertinentes comme par exemple les petites oscillations du pendule. Trop peu de candidats pensent à tracer et discuter des portraits de phase alors que l'intitulé de la leçon y invite clairement.

Il est possible d'évoquer les problématiques de l'approximation numérique dans cette leçon en présentant le point de vue du schéma d'Euler. On peut aller jusqu'à aborder la notion de problèmes raides et la conception de schémas implicites pour autant que le candidat ait une maîtrise convenable de ces questions.

221 Équations différentielles linéaires. Systèmes d'équations différentielles linéaires. Exemples et applications.

221.1 Développements

— 16 - Stabilité d'un système différentiel autonome.

— 27 - Étude d'une équation différentielle d'ordre 2 avec conditions au bord.

221.2 Rapport du Jury

Le jury attend d'un candidat qu'il sache déterminer rigoureusement la dimension de l'espace vectoriel des solutions. Le cas des systèmes à cœfficients constants fait appel à la réduction des matrices qui doit être connue et pratiquée. Le jury attend qu'un candidat puisse mettre en œuvre la méthode de variation des constantes pour résoudre une équation différentielle linéaire d'ordre 2 simple (à coefficients constants par exemple) avec second membre ; un trop grand nombre de candidats se trouve déstabilisés par ces questions.

L'utilisation des exponentielles de matrices a toute sa place ici et doit être maitrisée. Les problématiques de stabilité des solutions et le lien avec l'analyse spectrale devraient être exploitées.

Le théorème de Cauchy-Lipschitz linéaire constitue un exemple de développement pertinent pour cette leçon. Les résultats autour du comportement des solutions, ou de leurs zéros, de certaines équations linéaires d'ordre 2 (Sturm, Hill-Mathieu,...) sont aussi d'autres possibilités.

Pour aller plus loin, la résolution au sens des distributions d'équations du type $T' = 0$, ou des situations plus ambitieuses, trouvera sa place dans cette leçon.

223 Suites numériques. Convergence, valeurs d'adhérence. Exemples et applications.

223.1 Développements

— 32 - Critère de Weyl.

— 05 - Comportement asymptotique d'une suite à convergence lente.

223.2 Rapport du Jury

Cette leçon permet souvent aux candidats de s'exprimer. Il ne faut pas négliger les suites de nombres complexes mais les suites vectorielles (dans $\mathbb{R}^n$) ne sont pas dans le sujet. Le jury attire l'attention sur le fait que cette leçon n'est pas uniquement à consacrer à des suites convergentes, mais tout comportement asymptotique peut être présenté. Le théorème de Bolzano-Weierstrass doit être cité et le candidat doit être capable d'en donner une démonstration. On attend des candidats qu'ils parlent des limites inférieure et supérieure d'une suite réelle bornée, et qu'ils en maîtrisent le concept. Les procédés de sommation peuvent être éventuellement évoqués mais le théorème de Cesàro doit être mentionné et sa preuve maîtrisée par tout candidat à l'agrégation. Les résultats autour des sous-groupes additifs de $\mathbb{R}$ permettent d'exhiber des suites denses remarquables et l'ensemble constitue un joli thème. Des thèmes des leçons 225 (224 ?) et 226 peuvent également se retrouver dans cette leçon.

Pour aller plus loin, un développement autour de l'équirépartition est tout à fait envisageable. La méthode de Newton peut aussi illustrer la notion de vitesse de convergence.

224 Exemples de développements asymptotiques de suites et de fonctions.

224.1 Développements

— 15 - Méthode de Laplace.

— 05 - Comportement asymptotique d'une suite à convergence lente.

224.2 Rapport du Jury

Cette leçon doit permettre aux candidats d'exprimer leur savoir-faire sur les techniques d'analyse élémentaire que ce soit sur les suites, les séries ou les intégrales. On peut par exemple établir un développement asymptotique à quelques termes des sommes partielles de la série harmonique, ou bien la formule de Stirling que ce soit dans sa version factorielle ou pour la fonction Γ. On peut également s'intéresser aux comportements autour des singularités de fonctions spéciales célèbres. Du côté de l'intégration, on peut évaluer la vitesse de divergence de l'intégrale de la valeur absolue du sinus cardinal, avec des applications pour les séries de Fourier, voire présenter la méthode de Laplace.

Par ailleurs, le thème de la leçon permet l'étude de suites récurrentes (autres que le poncif $u_{n+1} = \sin(u_n)$), plus généralement de suites ou de fonctions définies implicitement, ou encore des études asymptotiques de solutions d'équations différentielles (sans résolution explicite).

On peut aller plus loin en abordant des techniques de phase stationnaire et en en discutant des applications.

226 Suites vectorielles et réelles définies par une relation de récurrence $u_{n+1} = f(u_n)$. Exemples. Applications à la résolution approchées d'équations.

226.1 Développements

— 19 - Méthode itérative de résolution de systèmes linéaires.

— 05 - Comportement asymptotique d'une suite à convergence lente.

226.2 Rapport du Jury

Citer au moins un théorème de point fixe est évidemment pertinent et savoir le mettre en oeuvre sur un exemple simple est indispensable. Le jury est toutefois surpris que des candidats évoquent un théorème de point fixe dans les espaces de Banach... sans être capables de définir ce qu'est un espace de Banach ou d'en donner un exemple ! On peut déjà commencer par énoncer un théorème de point fixe sur $\mathbb{R}$. Le jury attend d'autres exemples que la sempiternelle suite récurrente $u_{n+1} = \sin(u_n)$ (dont il est souhaitable de savoir expliquer les techniques sous-jacentes et le jury ne se privera pas de vérifier ce point sur un exercice). La notion de points attractifs ou répulsifs peut illustrer cette leçon. L'étude des suites linéaires récurrentes d'ordre p est souvent mal connue, notamment le lien avec l'aspect vectoriel, d'ailleurs ce dernier point est trop souvent négligé. Le comportement des suites vectorielles définies par une relation linéaire $X_{n+1} = AX_n$ fournit pourtant un matériel d'étude conséquent. La formulation de cette leçon invite résolument à évoquer les problématiques de convergence d'algorithmes (notamment savoir estimer la vitesse) d'approximation de solutions de problèmes linéaires et non linéaires : dichotomie, méthode de Newton (avec sa généralisation au moins dans $\mathbb{R}^2$), algorithme du gradient, méthode de la puissance, méthodes itératives de résolution de systèmes linéaires, schéma d'Euler,...

228 Continuité et dérivabilité des fonctions réelles d'une variable réelle. Exemples et applications.

228.1 Développements

— 27 - Utilisation de $H_0^1(0,1)$ pour étudier une équation différentielle.

— 15 - Méthode de Laplace.

228.2 Rapport du Jury

Cette leçon permet des exposés de niveaux très variés. Les théorèmes de base doivent être maîtrisés et illustrés par des exemples intéressants, par exemple le théorème des valeurs intermédiaires pour la dérivée. Le jury s'attend évidemment à ce que le candidat connaisse et puisse calculer la dérivée des fonctions usuelles. Les candidats doivent disposer d'un exemple de fonction dérivable de la variable réelle qui ne soit pas continûment dérivable. La stabilité par passage à la limite des notions de continuité et de dérivabilité doit être comprise par les candidats. De façon plus fine, on peut s'intéresser à des exemples de fonctions continues nulle part dérivables.

Les propriétés de régularité des fonctions convexes peuvent être mentionnées. Pour aller plus loin, la dérivabilité presque partout des fonctions lipschitziennes ou des fonctions monotones relève de cette leçon. L'étude des liens entre dérivée classique et dérivée au sens des distributions de fonctions telles que la fonction de Heaviside, de la valeur absolue ou de la fonction $x \mapsto \int_a^x f(y)dy$, f étant intégrable, peuvent trouver leur place dans cette leçon. On peut aussi relier la dérivée faible et la limite du taux d'accroissement au sens des distributions et établir le lien entre fonction croissante et dérivée faible positive.

229 Fonctions monotones. Fonctions convexes. Exemples et applications.

229.1 Développements

— 20 - Optimisation d'une fonctionnelle convexe dans un Hilbert.

— 03 - Une caractérisation de la fonction Γ.

229.2 Rapport du Jury

L'énoncé et la connaissance de la preuve de l'existence de limites à gauche et à droite pour les fonctions monotones sont attendues. Ainsi on doit parler des propriétés de continuité et de dérivabilité à gauche et à droite des fonctions convexes de la variable réelle. Il est souhaitable d'illustrer la présentation de la convexité par des dessins clairs. On notera que la monotonie concerne les fonctions réelles d'une seule variable réelle, mais que la convexité concerne également les fonctions définies sur une partie convexe de $\mathbb{R}^n$, qui fournissent de beaux exemples d'utilisation. L'étude de la fonctionnelle quadratique ou la minimisation de $\|Ax-b\|^2$ pourront illustrer agréablement cette leçon.

Pour aller plus loin, la dérivabilité presque partout des fonctions monotones est un résultat remarquable (dont la preuve peut être éventuellement admise). L'espace vectoriel engendré par les fonctions monotones (les fonctions à variation bornée) relève de cette leçon. Enfin, la dérivation au sens des distributions fournit les caractérisations les plus générales de la monotonie et de la convexité ; les candidats maîtrisant ces notions peuvent s'aventurer utilement dans cette direction.

230 Séries de nombres réels ou complexes. Comportement des restes ou des sommes partielles des séries numériques. Exemples.

230.1 Développements

— 31 - Théorème de convergence angulaire d'Abel et théorème Taubérien Faible.

— 22 - Formule sommatoire de Poisson, et application au calcul de $\zeta(2)$. $\rightarrow$ Nowp.

— 23 - Marche aléatoire symétrique sur $\mathbb{Z}^d$.

230.2 Rapport du Jury

De nombreux candidats commencent leur plan par une longue exposition des conditions classiques assurant la convergence ou la divergence des séries numériques. Sans être hors sujet, cette exposition ne doit pas former l'essentiel de la matière de la leçon. Un thème important de la leçon est en effet le comportement asymptotique des restes et sommes partielles (équivalents, développements asymptotiques — par exemple pour certaines suites récurrentes — cas des séries de Riemann, comparaison séries et intégrales,...). Le manque d'exemples est à déplorer.

On peut aussi s'intéresser à certaines sommes particulières, que ce soit pour exhiber des nombres irrationnels (voire transcendants), ou mettre en valeur des techniques de calculs non triviales (par exemple en faisant appel aux séries de Fourier ou aux séries entières).

Enfin, si le jury apprécie que le théorème des séries alternées (avec sa version sur le contrôle du reste) soit maîtrisé, il rappelle aussi que ses généralisations possibles utilisant la transformation d'Abel trouvent toute leur place dans cette leçon.

233 Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.

233.1 Développements

— 19 - Méthode itérative de résolution de systèmes linéaires.

— 13 - Méthode de Jacobi pour la recherche de valeurs propres de matrices symétriques réelles.

233.2 Rapport du Jury

Pour la session 2019, l'intitulé de cette leçon sera reformulé en

Analyse numérique matricielle : résolution approchée de systèmes linéaires, recherche de vecteurs propres, exemples.

[Cette leçon était auparavant intitulée

Méthodes itératives en analyse numérique matricielle].

Le jury reprend une formulation antérieure de l'intitulé car la leçon se focalisait trop exclusivement sur la résolution de systèmes linéaires par des méthodes itératives. Le jury souhaite un sujet plus ouvert et des propositions qui ne négligent plus la recherche de vecteurs propres et, de manière générale, l'exploitation de techniques d'analyse pour aborder la résolution approchée de systèmes linéaires et de leurs propriétés spectrales et approfondir la compréhension des algorithmes.

Dans cette leçon de synthèse, les notions de norme matricielle et de rayon spectral sont centrales, en lien avec le conditionnement et avec la convergence des méthodes itératives ; elles doivent être développées et maîtrisées. Le conditionnement d'une matrice symétrique définie positive doit être connu et un lien avec $\sup_{\|x\|=1} x^T Ax$ doit être fait. Le résultat général de convergence, relié au théorème du point fixe de Banach, doit être enrichi de considérations sur la vitesse de convergence.

Le jury invite les candidats à étudier diverses méthodes issues de contextes variés : résolution de systèmes linéaires, optimisation de fonctionnelles quadratiques (du type $\frac{1}{2}\langle Ax, x\rangle + \langle b, x\rangle$), recherche de valeurs propres,... Parmi les points intéressants à développer, on peut citer les méthodes de type Jacobi pour la résolution de systèmes linéaires, les méthodes de gradient dans le cadre quadratique, les méthodes de puissance et QR pour la recherche de valeurs propres. Les candidats pourront illustrer leur propos sur des matrices issues de schémas numériques pour les équations différentielles ou aux dérivées partielles linéaires.

236 Illustrer par des exemples quelques méthodes de calcul d'intégrales de fonctions d'une ou plusieurs variables.

236.1 Développements

— 15 - Méthode de Laplace.

— 11 - Transformée de Fourier d'une Gaussienne et inversion de Fourier.

236.2 Rapport du Jury

Cette leçon doit être très riche en exemples, que ce soit l'intégrale $\int_0^{+\infty} \frac{\sin(t)}{t} dt$ ou bien d'autres encore. Il est tout à fait pertinent de commencer par les différentes techniques élémentaires (intégration par parties, changement de variables, décomposition en éléments simples, intégrale à paramètres,...). On peut également présenter des utilisations du théorème des résidus, ainsi que des exemples faisant intervenir les intégrales multiples comme le calcul de l'intégrale d'une gaussienne. Le calcul du volume de la boule unité de $\mathbb{R}^n$ ne doit pas poser de problèmes insurmontables. Le calcul de la transformation de Fourier d'une gaussienne a sa place dans cette leçon.

On peut aussi penser à l'utilisation du théorème d'inversion de Fourier ou du théorème de Plancherel. Certains éléments de la leçon précédente, comme par exemple l'utilisation des théorèmes de convergence monotone, de convergence dominée et/ou de Fubini, sont aussi des outils permettant le calcul de certaines intégrales.

Enfin, il est tout à fait pertinent d'évoquer les méthodes de calcul approché d'intégrales (méthodes des rectangles, méthode de Monte-Carlo, etc.).

239 Fonctions définies par une intégrale dépendant d'un paramètre. Exemples et applications.

239.1 Développements

— 15 - Méthode de Laplace.

— 03 - Une caractérisation de la fonction Γ.

— 11 - Transformée de Fourier d'une Gaussienne et inversion de Fourier.

239.2 Rapport du Jury

Les candidats incluent les théorèmes de régularité (version segment — a minima — mais aussi version « convergence dominée ») ce qui est pertinent mais la leçon ne doit pas se réduire seulement à cela. Cette leçon doit être riche en exemples, ce qui parfois n'est pas suffisamment le cas, et peut être encore enrichie par des études et méthodes de comportements asymptotiques. Les propriétés de la fonction Γ d'Euler fournissent un développement standard, mais non sans risque (on pourra y inclure le comportement asymptotique, voire son prolongement analytique) ; certains candidats sont trop ambitieux pour le temps dont ils disposent. Le jury invite donc à bien préciser ce que le candidat souhaite montrer pendant son développement. Les différentes transformations classiques (Fourier, Laplace,...) relèvent aussi naturellement de cette leçon. On peut en donner des applications pour obtenir la valeur d'intégrales classiques (celle de l'intégrale de Dirichlet par exemple). Le théorème d'holomorphie sous le signe intégrale est trop peu souvent cité.

Pour aller encore plus loin, on peut par exemple développer les propriétés des transformations mentionnées (notamment la transformée de Fourier, par exemple en s'attardant sur le lien entre régularité de la fonction et décroissance de sa transformée de Fourier), ainsi que de la convolution.

243 Convergence des séries entières, propriétés de la somme. Exemples et applications.

243.1 Développements

— 01 - Dénombrement des partitions d'un ensemble fini par les séries entières.

— 31 - Théorème de convergence Angulaire d'Abel et théorème taubérien faible.

243.2 Rapport du Jury

Les candidats évoquent souvent des critères (Cauchy, D'Alembert) permettant d'estimer le rayon de convergence mais oublient souvent la formule de Cauchy-Hadamard ou toute technique utilisant une majoration ou un équivalent. Le jury attend bien sûr que le candidat puisse donner des arguments justifiant qu'une série entière en 0 dont le rayon de convergence est R est développable en série entière en un point z_0 intérieur au disque de convergence et de minorer le rayon de convergence de cette série. Sans tomber dans un catalogue excessif, on peut indiquer les formules de développement de fonctions usuelles importantes $(\exp, \log, 1/(1-z), \sin, \dots)$. S'agissant d'exemples fondamentaux et classiques, le jury attend que le candidat puisse les donner sans consulter ses notes. En ce qui concerne la fonction exponentielle, le candidat doit avoir réfléchi au point de vue adopté sur sa définition et donc sur l'articulation entre l'obtention du développement en série entière et les propriétés de la fonction. À ce propos, les résultats sur l'existence du développement en série entière pour les fonctions dont on contrôle toutes les dérivées successives sur un voisinage de 0 sont souvent méconnus. Le comportement de la série entière dans le disque de convergence vis à vis des différents modes de convergence (convergence absolue, convergence uniforme, convergence normale) doit être maîtrisé.

Le théorème d'Abel (radial ou sectoriel) trouve toute sa place mais doit être agrémenté d'exercices pertinents. Réciproquement, les théorèmes taubériens offrent aussi de jolis développements. On pourra aller plus loin en abordant quelques propriétés importantes liées à l'analyticité de la somme d'une série entière ou encore la résolution de certaines équations différentielles ordinaires par la méthode du développement en série entière.

246 Séries de Fourier. Exemples et applications.

246.1 Développements

— 22 - Formule sommatoire de Poisson.

— 23 - Marche aléatoire symétrique sur $\mathbb{Z}^d$.

246.2 Rapport du Jury

Les différents résultats autour de la convergence (L^2, Fejér, Dirichlet, . . .) doivent être connus. On prendra garde au sens de la notation $\sum_{n\in\mathbb{Z}}$ (qu'il est plus prudent d'éviter car elle est souvent inadaptée). Il faut avoir les idées claires sur la notion de fonctions de classe C^1 par morceaux (elles ne sont pas forcément continues). Le théorème d'isométrie bijective entre espaces L^2 et ℓ^2 doit apparaitre. Dans le cas d'une fonction continue et C^1 par morceaux on peut conclure sur la convergence normale de la série Fourier sans utiliser le théorème de Dirichlet. Il est classique d'obtenir des sommes de séries remarquables comme conséquence de ces théorèmes.

On peut aussi s'intéresser à la formule de Poisson et à ses conséquences. L'existence d'exemples de séries de Fourier divergentes, associées à des fonctions continues (qu'ils soient explicites ou obtenus par des techniques d'analyse fonctionnelle) peuvent aussi compléter le contenu.

Il est souhaitable que cette leçon ne se réduise pas à un cours abstrait sur les cœfficients de Fourier. La résolution d'équations aux dérivées partielles (par exemple l'équation de la chaleur ou l'équation des ondes avec une estimation de la vitesse de convergence) peut illustrer de manière pertinente cette leçon, mais on peut penser à bien d'autres applications (inégalité isopérimétrique, comportements remarquables des fonctions à spectre lacunaire,...).

250 Transformation de Fourier. Applications.

250.1 Développements

— 11 - Théorème d'inversion de Fourier.

— 22 - Formule sommatoire de Poisson.

250.2 Rapport du Jury

Cette leçon offre de multiples facettes. Les candidats peuvent adopter différents points de vue : L^1, L^2, et/ou distributions. L'aspect « séries de Fourier » n'est toutefois pas dans l'esprit de cette leçon ; il ne s'agit pas de faire de l'analyse de Fourier sur n'importe quel groupe localement compact mais sur $\mathbb{R}$ ou $\mathbb{R}^d$.

La leçon nécessite une bonne maîtrise de questions de base telle que la définition du produit de convolution de deux fonctions de L^1. En ce qui concerne la transformation de Fourier, elle ne doit pas se limiter à une analyse algébrique de la transformation de Fourier. C'est bien une leçon d'analyse, qui nécessite une étude soigneuse des hypothèses, des définitions et de la nature des objets manipulés. Le lien entre la régularité de la fonction et la décroissance de sa transformée de Fourier doit être fait, même sous des hypothèses qui ne sont pas minimales. Les candidats doivent savoir montrer le lemme de Riemann-Lebesgue pour une fonction intégrable.

La formule d'inversion de Fourier pour une fonction L^1 dont la transformée de Fourier est aussi L^1 est attendue ainsi que l'extension de la transformée de Fourier à l'espace L^2 par Fourier-Plancherel. Des exemples explicites de calcul de transformations de Fourier, classiques comme la gaussienne ou $(1+x^2)^{-1}$, paraissent nécessaires.

Pour aller plus loin, la transformation de Fourier des distributions tempérées ainsi que la convolution dans le cadre des distributions tempérées peuvent être abordées. Rappelons une fois de plus que les attentes du jury sur ces questions restent modestes, au niveau de ce qu'un cours de première année de master sur le sujet peut contenir. Le fait que la transformée de Fourier envoie $S(\mathbb{R}^d)$ dans lui même avec de bonnes estimations des semi-normes doit alors être compris et la formule d'inversion de Fourier maîtrisée dans ce cadre. Des exemples de calcul de transformée de Fourier peuvent être donnés dans des contextes liés à la théorie des distributions comme par exemple la transformée de Fourier de la valeur principale. Dans un autre registre, il est aussi possible d'orienter la leçon vers l'étude de propriétés de fonctions caractéristiques de variables aléatoires.

La résolution de certaines équations aux dérivées partielles telles que, par exemple, l'équation de la chaleur sur $\mathbb{R}$, peut être abordée, avec une discussion sur les propriétés qualitatives des solutions.

260 Espérance, variance et moments d'une variable aléatoire.

260.1 Développements

— 26 - Convergence de séries de variables aléatoires.

— 23 - Marche aléatoire dans $\mathbb{Z}^d$.

260.2 Rapport du Jury

Le jury attend des candidats qu'ils donnent la définition des moments centrés, qu'ils rappellent les implications d'existence de moments (décroissance des L^p). Les variables aléatoires à densité sont trop souvent négligées. Le candidat peut citer — mais doit surtout savoir retrouver rapidement — les espérances et variances de lois usuelles, notamment Bernoulli, binomiale, géométrique, Poisson, exponentielle, normale. La variance de la somme de variables aléatoires indépendantes suscite souvent des hésitations. Les inégalités classiques (de Markov, de Bienaymé-Chebyshev, de Jensen et de Cauchy-Schwarz) pourront être données, ainsi que les théorèmes de convergence (lois des grands nombres et théorème central limite). La notion de fonction génératrice des moments pourra être présentée ainsi que les liens entre moments et fonction caractéristique.

Pour aller plus loin, le comportement des moyennes empiriques pour une suite de variables aléatoires indépendantes et identiquement distribuées n'admettant pas d'espérance pourra être étudié. Pour les candidats suffisamment à l'aise avec ce sujet, l'espérance conditionnelle pourra aussi être abordée.

264 Variables aléatoires discrètes. Exemples et applications.

264.1 Développements

— 26 - Convergence de séries de variables aléatoires.

— 23 - Marche aléatoire dans $\mathbb{Z}^d$.

264.2 Rapport du Jury

Le jury attend des candidats qu'ils rappellent la définition d'une variable aléatoire discrète et que des lois usuelles soient présentées, en lien avec des exemples classiques de modélisation. Le lien entre variables aléatoires de Bernoulli, binomiale et de Poisson doit être discuté. Il peut être d'ailleurs intéressant de mettre en avant le rôle central joué par les variables aléatoires de Bernoulli.

Les techniques spécifiques aux variables discrètes, notamment à valeurs entières, devront être mises en évidence, comme par exemple la caractérisation de la convergence en loi, la notion de fonction génératrice.

Pour aller plus loin, le processus de Galton-Watson peut se traiter intégralement à l'aide des fonctions génératrices et cette voie a été choisie par plusieurs candidats : cela donne un développement de très bon niveau pour ceux qui savent justifier les étapes délicates.

Pour aller beaucoup plus loin, les candidats pourront étudier les marches aléatoires, les chaînes de Markov à espaces d'états finis ou dénombrables, les sommes ou séries de variables aléatoires indépendantes.

265 Exemples d'études et d'applications de fonctions usuelles et spéciales.

265.1 Développements

265.2 Rapport du Jury

Cette leçon est très riche ; c'est une leçon de synthèse qui doit permettre d'explorer de nombreux pans du programme. Évidemment, la leçon ne doit pas se cantonner au seul champ des fonctions usuelles (logarithme, exponentielle, trigonométriques, hyperboliques et réciproques). Le jury attend surtout d'un agrégé qu'il soit en mesure de présenter rapidement les définitions et les propriétés fondamentales de ces fonctions, qu'il sache les tracer sans difficultés, qu'il puisse mener l'étude aux bornes de leur domaine, ainsi que discuter leurs prolongements éventuels, leurs développements de Taylor ou en série entière, leurs applications au calcul intégral, les équations fonctionnelles associées ou formules particulières, etc. Le jury n'attend pas un catalogue mais plutôt un choix pertinent et réfléchi, avec des applications en probabilité, convexité, études de courbes, ou autour des développements asymptotiques. Les déterminations du logarithme complexe peuvent tout à fait mériter une discussion approfondie dans cette leçon et donner lieu à des développements de bon niveau, pouvant aller jusqu'à leur interprétation géométrique.

Le domaine des fonctions spéciales est très vaste. Il faut absolument éviter l'écueil d'une taxonomie fastidieuse et dépourvue de motivation ; il vaut bien mieux se concentrer sur des exemples restreints, mais fouillés, par exemple une étude approfondie (d'une) des fonctions Γ, ζ ou θ, leurs propriétés fonctionnelles, leurs prolongements, leur étude asymptotique aux bornes et les domaines d'applications de ces fonctions.

Il y a donc bien des manières, très différentes, de construire valablement cette leçon. Par exemple, on peut bâtir un exposé organisé selon des problématiques et des techniques mathématiques : suites et séries de fonctions, fonctions holomorphes et méromorphes, problèmes de prolongement, développements asymptotiques, calculs d'intégrales et intégrales à paramètres, transformées de Fourier ou de Laplace, etc. Mais on pourrait tout aussi bien suivre un fil conducteur motivé par un domaine d'application :

- en arithmétique pour évoquer, par exemple, la fonction ζ et la distribution des nombres premiers,
- en probabilités où la loi normale et la fonction erreur sont évidemment incontournables mais on peut aussi évoquer les lois Gamma et Bêta, les fonctions de Bessel et leurs liens avec la densité du χ^2 non centrée et celle de la distribution de Von Mises-Fisher ou plus simplement comme loi du produit de variables aléatoires normales et indépendantes, la loi ζ et ses liens avec la théorie des nombres,...
- en analyse des équations aux dérivées partielles où les fonctions spéciales interviennent notamment pour étudier le problème de Dirichlet pour le Laplacien ou l'équation des ondes,
- il est aussi possible d'évoquer les polynômes orthogonaux, leurs propriétés et leurs diverses applications, en physique (oscillateur harmonique et polynômes de Hermite), en probabilités (polynômes de Hermite pour les lois normales, de Laguerre pour les lois Gamma, de Jacobi pour les lois Bêta...), pour l'étude d'équations aux dérivées partielles ou pour l'analyse de méthodes numériques,
- en théorie des représentations de groupes avec les fonctions de Bessel,

— en algèbre en abordant les fonctions p-elliptiques.

Là encore, le jury renouvelle sa mise en garde d'éviter de faire un catalogue qui s'avérerait stérile, il s'agit bien plutôt de se tenir à détailler l'un ou l'autre de ces points de vue. Au final, cette leçon peut être l'occasion de montrer un véritable investissement personnel, adossé aux goûts du candidat.

CHAPITRE 8

INFO

901 Structures de données. Exemples et applications.

901.1 Développements :

— 07 - Coût amorti des arbres 2-4.

— 11 - Hachage Parfait.

901.2 Rapport de Jury

Le mot algorithme ne figure pas dans l'intitulé de cette leçon, même si l'utilisation des structures de données est évidemment fortement liée à des questions algorithmiques. La leçon doit donc être orientée plutôt sur la question du choix d'une structure de données. Le jury attend du candidat qu'il présente différents types abstraits de structures de données en donnant quelques exemples de leur usage avant de s'intéresser au choix de la structure concrète. Le candidat ne peut se limiter à des structures linéaires simples comme des tableaux ou des listes, mais doit présenter également quelques structures plus complexes, reposant par exemple sur des implantations à l'aide d'arbres. Les notions de complexité des opérations usuelles sur la structure de données sont bien sûr essentielles dans cette leçon.

903 Exemples d'algorithmes de tri. Correction et complexité.

903.1 Développements :

— 19 - Complexité du tri rapide avec pivot aléatoire.

— 22 - Tris en temps linéaire.

903.2 Rapport de Jury

Sur un thème aussi classique, le jury attend des candidats la plus grande précision et la plus grande rigueur. Ainsi, sur l'exemple du tri rapide, il est attendu du candidat qu'il sache décrire avec soin l'algorithme de partition et en prouver la correction en exhibant un invariant adapté. L'évaluation des complexités dans le cas le pire et en moyenne devra être menée avec rigueur : si on utilise le langage des probabilités, il importe que le candidat sache sur quel espace probabilisé il travaille. On attend également du candidat qu'il évoque la question du tri en place, des tris stables, des tris externes ainsi que la représentation en machine des collections triées.

907 Algorithmique du texte. Exemples et applications.

907.1 Références

— Crochemore Algorithm on strings

— Crochemore Jewels of stringology

— Beauquier-chretienne (KMP, Boyer-Moore, MP etc)

907.2 Remarques générales

— Grep d'unix utilise Boyer-Moore quand il n'y a qu'une seule string, mais aho-corasick sinon.

— C'est très bien de mettre d'autres algo du texte que la recherche de motif. Distance d'édition ok, compression encore mieux (tant que ça reste dans le sujet).

— Dans le plan on peut mettre une partie d'ouverture à la fin, ou bien en conclusion, pour parler d'analyse lexicale et syntaxique.

— Concernant les coût, c'est sans doute mieux dans une leçon d'agreg de mettre un coût élémentaire de 1.

— Mettre plein de dessins.

907.3 Développements :

— 03 - Algorithme d'Aho Corasick pour la recherche de motifs.

— 09 - Distance d'édition.

907.4 Rapport de Jury

Cette leçon devrait permettre au candidat de présenter une grande variété d'algorithmes et de paradigmes de programmation, et ne devrait pas se limiter au seul problème de la recherche d'un motif dans un texte, surtout si le candidat ne sait présenter que la méthode naïve.

De même, des structures de données plus riches que les tableaux de caractères peuvent montrer leur utilité dans certains algorithmes, qu'il s'agisse d'automates ou d'arbres par exemple.

Cependant, cette leçon ne doit pas être confondue avec la 909, « Langages rationnels et Automates finis. Exemples et applications. ». La compression de texte peut faire partie de cette leçon si les algorithmes présentés contiennent effectivement des opérations comme les comparaisons de chaînes : la compression LZW, par exemple, est plus pertinente dans cette leçon que la compression de Huffman.

907.5 Leçon

Aaron : Texte format omniprésent pour manipuler des données, et en particulier en bioinformatique.

Part I : Définitions et prérequis 1) Implémentation des automates et complexité.

Tableau comparaison complexité.

Part II : Recherche de motif dans un texte Algo naif quadratique –> optimisation

1) Morris-Pratt : Déplacer une fenêtre –> O(|T|)
2) KMP : Prétraitement plus fin qui permet d'être plus efficace.
3) Aho-Corasik (premier dev)
4) Boyer-Moore = Famille d'algorithme. On change le sens de lecture du texte (GD –> DG)
Part III : Calcul de la distance d'édition
Algo dynamique = >Dev 2<
Part IV : Algo de compression de texte.
Lempel-Ziv

907.6 Questions sur le Dev

Dev choisi : Distance d'édition. Présentation de l'algo "avec les mains" + faire tourner sur un exemple.

Questions

- Réexpliquer l'algo
- Complexité ? Temps ? Espace ? Optimisation ? –> Algo Diviser Pour régner dans le [Tardos & al]
- Graphe d'édition –> Plus court chemin.
- Reformaliser la correction de l'algorithme.
- Remarque sur l'algo : Si on ne fait pas attention au coût des opérations élémentaires on peut avoir des surprises : Par exemple si

$$Ins(\varepsilon, c) + Sub(c, a) < Ins(\varepsilon, a)$$

et pourtant aurait le même résultat ! Il faut donc rajouter des hypothèses.

> **Note :** On revient à ma définition de distance d'édition comme longueur minimale des dérivations !

- La complexité de l'algo donné tel quel ne dépend que des longueurs des instances, pas des instances elles-mêmes. Peut-on améliorer l'algo on se servant des spécificités des entrées ?
- Pourquoi l'hypothèse d'avoir
- On se donne un type abstrait char. Qu'est-ce que le type abstrait String ? Qu'est-ce qu'une bonne implémentation ?
- Application de la distance d'édition ? ADN. Plus informatique ? Détecter un plagiat.

907.7 Questions plan

- Via un schéma voir la différence entre MP, KMP & co.

907.8 Questions classiques

- Algo utilisé par grep ? –> Boyer-Moore (pattern unique) ou Aho-Corasick (plusieurs patterns (fixés))
- Exemple de pire cas pour les algos du plan.

909 Langages rationnels et Automates finis. Exemples et applications.

909.1 Développements :

— 03 - Algorithme d'Aho Corasick pour la recherche de motifs.

— 18 - Décidabilité de l'arithmétique de Presburger.

909.2 Rapport de Jury

Pour cette leçon très classique, il importe de ne pas oublier de donner exemples et applications, ainsi que le demande l'intitulé.

Une approche algorithmique doit être privilégiée dans la présentation des résultats classiques (déterminisation, théorème de Kleene, etc.) qui pourra utilement être illustrée par des exemples. Le jury pourra naturellement poser des questions telles que : connaissez-vous un algorithme pour décider de l'égalité des langages reconnus par deux automates ? quelle est sa complexité ?

Des applications dans le domaine de l'analyse lexicale et de la compilation entrent naturellement dans le cadre de cette leçon.

912 Fonctions récursives primitives et non primitives. Exemples.

912.1 Développements :

— 02 - La fonction d'Ackerman n'est pas récursive primitive.

— 16 - Équivalence entre les Machines de Turing et les fonctions récursives.

— ?? - Équivalence entre les fonctions récursives et le lambda-calcul.

912.2 Rapport de Jury

Il s'agit de présenter un modèle de calcul : les fonctions récursives. S'il est bien sûr important de faire le lien avec d'autres modèles de calcul, par exemple les machines de Turing, la leçon doit traiter des spécificités de l'approche. Le candidat doit motiver l'intérêt de ces classes de fonctions sur les entiers et pourra aborder la hiérarchie des fonctions récursives primitives. Enfin, la variété des exemples proposés sera appréciée.

913 Machines de Turing. Applications.

913.1 Développements :

— 16 - Équivalence entre les Machines de Turing et les fonctions récursives.

— 12 - Théorème de Hierarchie en espace et en temps.

913.2 Rapport de Jury

Il s'agit de présenter un modèle de calcul. Le candidat doit expliquer l'intérêt de disposer d'un modèle formel de calcul et discuter le choix des machines de Turing. La leçon ne peut se réduire à la leçon 914 ou à la leçon 915, même si, bien sûr, la complexité et l'indécidabilité sont des exemples d'applications. Plusieurs développements peuvent être communs avec une des leçons 914, 915, mais il est apprécié qu'un développement spécifique soit proposé.

914 Décidabilité et indécidabilité. Exemples.

914.1 Développements :

— 18 - Décidabilité de l'arithmétique de Presburger.

— 10 - Indécidabilité et grammaires algébriques.

914.2 Rapport de Jury

Le programme de l'option offre de très nombreuses possibilités d'exemples. Si les exemples classiques de problèmes sur les machines de Turing figurent naturellement dans la leçon, le jury apprécie des exemples issus d'autres parties du programme : théorie des langages, logique,... Le jury portera une attention particulière à une formalisation propre des réductions, qui sont parfois très approximatives.

915 Classes de complexité. Exemples.

915.1 Développements :

— 01 - 2-SAT est NL-Complet.

— 12 - Théorème de Hierarchie en espace et en temps.

915.2 Rapport de Jury

Le jury attend que le candidat aborde à la fois la complexité en temps et en espace. Il faut naturellement exhiber des exemples de problèmes appartenant aux classes de complexité introduites, et montrer les relations d'inclusion existantes entre ces classes, en abordant le caractère strict ou non de ces inclusions. Le jury s'attend à ce que les notions de réduction polynomiale, de problème complet pour une classe, de robustesse d'une classe vis à vis des modèles de calcul soient abordées.

Se focaliser sur la décidabilité dans cette leçon serait hors sujet.

916 Formules du calcul propositionnel : représentation, formes normales, satisfiabilité. Applications.

916.1 Développements :

— 20 - Complétude de la résolution.

— 01 - 2SAT est NL complet + temps polynomial.

916.2 Rapport de Jury

Le jury attend des candidats qu'ils abordent les questions de la complexité de la satisfiabilité. Pour autant, les applications ne sauraient se réduire à la réduction de problèmes NP-complets à SAT. Une partie significative du plan doit être consacrée à la représentation des formules et à leurs formes normales.

916.3 Références

http ://www.lsv.fr/ goubault/resolfidx.html

— Goubault-Mackie [GLM97] chapitre 2.

— Autebert ?

— Lalement.

916.4 Métaplan

Idée : On suit le titre de la leçon. On fait une partie sur la définition de la logique propositionnelle, syntaxe, sémantique, satisfiabilité. On dit que SAT est NP-Complet. Puis on introduit les formes normales : nnf, cnf, dnf avec les complexités associées et des exemples. On peut parler de systèmes complets de connecteurs booléens, et le lien avec le hardware. On conclut cette partie en parlant des BDD de Shannon, la forme normale par excellence. Puis on fait une troisième partie sur la satisfiabilité. Une formule est insatisfiable si son complémentaire est valide. Systèmes de preuve, résolution (Complétude réfutationnelle de la résolution >DEV<). On peut en déduire le théorème de compacité. Variante de SAT : 2SAT est NL-complet, et temps polynomial >DEV<).

918 Systèmes formels de preuve en logique du premier ordre. Exemples.

http ://www.lsv.fr/ goubault/resolfidx.html

918.1 Développements :

— 14 - Une preuve formelle en logique du premier ordre.

— 17 - Complétude de la déduction naturelle.

918.2 Rapport de Jury

Le jury attend du candidat qu'il présente au moins la déduction naturelle ou un calcul de séquents et qu'il soit capable de développer des preuves dans ce système sur des exemples classiques simples. La présentation des liens entre syntaxe et sémantique, en développant en particulier les questions de correction et complétude, et de l'apport des systèmes de preuves pour l'automatisation des preuves est également attendue.

Le jury appréciera naturellement si des candidats présentent des notions plus élaborées comme la stratégie d'élimination des coupures mais est bien conscient que la maîtrise de leurs subtilités va au-delà du programme.

921 Algorithmes de recherche et structures de données associées.

921.1 Développements :

— 11 - Hachage Parfait.

— 07 - Coût amorti des arbres 2-4.

921.2 Rapport de Jury

Le sujet de la leçon concerne essentiellement les algorithmes de recherche pour trouver un élément dans un ensemble : l'intérêt des structures de données proposées et de leur utilisation doit être argumenté dans ce contexte.

La recherche d'une clé dans un dictionnaire sera ainsi par exemple l'occasion de définir la structure de données abstraite « dictionnaire », et d'en proposer plusieurs implantations concrètes. De la même façon, on peut évoquer la recherche d'un mot dans un lexique : les arbres préfixes (ou digital tries) peuvent alors être présentés. Mais on peut aussi s'intéresser à des domaines plus variés, comme la recherche d'un point dans un nuage (et les quad-trees), et bien d'autres encore.

923 Analyse lexicale et syntaxique. Applications.

923.1 Développements :

— 05 - Analyse LL(1) sur un exemple.

— 10 - Indécidabilité et grammaires algébriques.

923.2 Rapport de Jury

Cette leçon ne doit pas être confondue avec la 909, qui s'intéresse aux seuls langages rationnels, ni avec la 907, sur l'algorithmique du texte.

Si les notions d'automates finis et de langages rationnels et de grammaires algébriques sont au cœur de cette leçon, l'accent doit être mis sur leur utilisation comme outils pour les analyses lexicale et syntaxique. Il s'agit donc d'insister sur la différence entre langages rationnels et algébriques, sans perdre de vue l'aspect applicatif : on pensera bien sûr à la compilation. Le programme permet également des développements pour cette leçon avec une ouverture sur des aspects élémentaires d'analyse sémantique.

923.3 Remarques

— Le système de typage du langage Pascal est fondé sur une grammaire $LL(1)$.

— L'analyse descendante LL n'est pas très efficace et on peut faire plus de choses avec une analyse ascendante LR qui se fait à l'aide d'une pile (–> Automate à pile).

— En pratique, les langages de programmations actuels possèdent une grammaire dite LALR.

924 Théories et modèles en logique du premier ordre. Exemples.

924.1 Développements :

— 18 - Décidabilité de l'Arithmétique de Presburger.

— 17 - Complétude de la déduction naturelle.

924.2 Rapport de Jury

Le jury s'attend à ce que la leçon soit abordée dans l'esprit de l'option informatique, en insistant plus sur la décidabilité/indécidabilité des théories du premier ordre que sur la théorie des modèles.

Il est attendu que le candidat donne au moins un exemple de théorie décidable (respectivement complète) et un exemple de théorie indécidable.

Le jury appréciera naturellement si des candidats connaissent l'existence du premier théorème d'incomplétude mais est bien conscient que la démonstration va au-delà du programme.

924.3 Exemples, contre exemples

— Une théorie qui possède un modèle fini est-elle décidable ? → Non, la théorie des groupes est indécidable.

— Le théorème de compacité est faux dans le monde des modèles finis : En effet, pour $n \in \mathbb{N}$ posons

$$\theta_n := \exists x_1, \dots, x_n \left(\left(\bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \right) \bigwedge \left(\forall x \bigvee_{1 \leq i \leq n} x = x_i \right) \right)$$

et considérons

$$T := \{\neg \theta_n \mid n \in \mathbb{N}\}$$

Alors, pour tout n, $\mathcal{M} \vDash \theta_n$ ssi $|\mathcal{M}| = n$. En particulier, tout sous ensemble fini de T possède un modèle fini, mais T n'a aucun modèle fini.

925 Graphes : représentations et algorithmes.

925.1 Développements :

— 15 - Algorithme de Kruskal.

— 01 - 2SAT est NL complet + temps polynomial.

925.2 Rapport de Jury

Cette leçon offre une grande liberté de choix au candidat, qui peut choisir de présenter des algorithmes sur des problèmes variés : connexité, diamètre, arbre couvrant, flot maximal, plus court chemin, cycle eulérien, etc. mais aussi des problèmes plus difficiles, comme la couverture de sommets ou la recherche d'un cycle hamiltonien, pour lesquels il pourra proposer des algorithmes d'approximation ou des heuristiques usuelles. Une preuve de correction des algorithmes proposés sera évidemment appréciée. Il est attendu que diverses représentations des graphes soient présentées et comparées, en particulier en termes de complexité.

925.3 Exemples, applications

— Le tri topologique est utilisé par le logiciel Make pour résoudre des dépendances.

926 Analyse des algorithmes : complexité. Exemples.

926.1 Développements :

— 07 - Coût amorti des arbres 2-4.

— 19 - Complexité du tri rapide avec pivot aléatoire.

926.2 Rapport de Jury

Il s'agit ici d'une leçon d'exemples. Le candidat prendra soin de proposer l'analyse d'algorithmes portant sur des domaines variés, avec des méthodes d'analyse également variées : approche combinatoire ou probabiliste, analyse en moyenne ou dans le pire cas. Si la complexité en temps est centrale dans la leçon, la complexité en espace ne doit pas être négligée. La notion de complexité amortie a également toute sa place dans cette leçon, sur un exemple bien choisi, comme union find (ce n'est qu'un exemple).

927 Exemples de preuve d'algorithme : Correction, terminaison.

927.1 Développements :

— 15 - Algorithme de Kruskal.

— 13 - Une preuve en Hoare.

927.2 Rapport de Jury

Le jury attend du candidat qu'il traite des exemples d'algorithmes récursifs et des exemples d'algorithmes itératifs.

En particulier, le candidat doit présenter des exemples mettant en évidence l'intérêt de la notion d'invariant pour la correction partielle et celle de variant pour la terminaison des segments itératifs.

Une formalisation comme la logique de HOARE pourra utilement être introduite dans cette leçon, à condition toutefois que le candidat en maîtrise le langage. Des exemples non triviaux de correction d'algorithmes seront proposés. Un exemple de raisonnement type pour prouver la correction des algorithmes gloutons pourra éventuellement faire l'objet d'un développement.

928 Problèmes NP-Complets : exemples et réductions.

928.1 Développements :

— 08 - L'inclusion de requêtes conjonctives est NP-Complet.

— 04 - Algo d'approximation.

928.2 Rapport de Jury

L'objectif ne doit pas être de dresser un catalogue le plus exhaustif possible ; en revanche, pour chaque exemple, il est attendu que le candidat puisse au moins expliquer clairement le problème considéré, et indiquer de quel autre problème une réduction permet de prouver sa NP-complétude. Les exemples de réduction polynomiale seront autant que possible choisis dans des domaines variés : graphes, arithmétique, logique, etc. Si les dessins sont les bienvenus lors du développement, le jury attend une définition claire et concise de la fonction associant, à toute instance du premier problème, une instance du second ainsi que la preuve rigoureuse que cette fonction permet la réduction choisie et que les candidats sachent préciser comment sont représentées les données.

Un exemple de problème NP-complet dans sa généralité qui devient P si on contraint davantage les hypothèses pourra être présenté, ou encore un algorithme P approximant un problème NP-complet.

928.3 Leçon de Kang

Rmq 25 : Sat est le premier probleme NP-Complet –> Pas sûr.

Devs = Cook (Choisi) et "Si $P \neq NP$, pour tout $\rho \geq 1$ constante, il n'existe pas de ρ-approximation en temps polynomial du probleme du voyageur de commerce."

928.4 Questions sur le Dev

Dev long (17').

— Préciser un point du développement.

— Preuve "haut niveau" de $\varphi_\omega \in SAT \Rightarrow \omega \in L$?

— Ça veut dire quoi que $\mathcal{M}$ travaille en temps $p(n)$?

— Dans le plan il faut définir la notion de machine de turing et de temps d'execution qu'on utilise. On peut parler de timeout etc. Ça permet d'éviter les questions tordues sur les notions de machines.

— Réduction pas constructible. Est-ce grave ? → Non, on montre juste qu'il existe une réduction.

— Là on a un alphabet fini. Si on permet un alphabet infini contenant $\mathbb{Z}$ pour permettre à la machine de faire des incréments a-t-on la même notion ? Oui on s'en fout on peut borner les lettres qu'on utilise puisqu'on borne la taille de l'execution.

— Si la table de transition ne dépend pas uniquement de la lettre courante, mais également d'une fenetre. Est-ce que ça serait NP-complet ?

928.5 Questions sur le plan

— Il existe des classes C de complexité telle qu'aucun probleme C-complet soit connu.

— Définitions dans les problemes, type cycle hamiltonien etc.

— Donner un exemple pour utiliser SAT.

— Si on change la notion de réduction polynomiale en réduction en temps ND polynomial, est-ce que ça change les problèmes ? $\rightarrow$ Oui tous les problemes de NP deviennent NP difficiles.

929 Lambda-Calcul pur comme modèle de calcul. Exemples.

929.1 Développements :

— **??** - Confluence de la β-réduction.

— **??** - Équivalence entre les fonctions récursives et le lambda-calcul.

929.2 Rapport de Jury

Il s'agit de présenter un modèle de calcul : le lambda-calcul pur. Il est important de faire le lien avec au moins un autre modèle de calcul, par exemple les machines de Turing ou les fonctions récursives.

Néanmoins, la leçon doit traiter des spécificités du lambda-calcul. Ainsi le candidat doit motiver l'intérêt du lambda-calcul pur sur les entiers et pourra aborder la façon dont il permet de définir et d'utiliser des types de données (booléens, couples, listes, arbres).

930 Sémantique des langages de programmation. Exemples.

930.1 Développements :

— 21 - Equivalences de sémantiques.

— 13 - Une preuve en Hoare.

930.2 Rapport de Jury

L'objectif est de formaliser ce qu'est un programme : introduction des sémantiques opérationnelle et dénotationnelle, dans le but de pouvoir faire des preuves de programmes, des preuves d'équivalence, des preuves de correction de traduction.

Ces notions sont typiquement introduites sur un langage de programmation (impératif) jouet. On peut tout à fait se limiter à un langage qui ne nécessite pas l'introduction des CPOs et des théorèmes de point fixe généraux. En revanche, on s'attend ici à ce que les liens entre sémantique opérationnelle et dénotationnelle soient étudiés (toujours dans le cas d'un langage jouet). Il est aussi important que la leçon présente des exemples d'utilisation des notions introduites, comme des preuves d'équivalence de programmes ou des preuves de correction de programmes.

931 Schémas algorithmiques. Exemples et applications.

931.1 Développements :

— 04 - Un algo d'approximation.

— 09 - Distance d'édition.

931.2 Rapport de Jury

Cette leçon permet au candidat de présenter différents schémas algorithmiques, en particulier « diviser pour régner », programmation dynamique et approche gloutonne. Le candidat pourra choisir de se concentrer plus particulièrement sur un ou deux de ces paradigmes. Le jury attend du candidat qu'il illustre sa leçon par des exemples variés, touchant des domaines différents et qu'il puisse discuter les intérêts et limites respectifs des méthodes. Le jury ne manquera pas d'interroger plus particulièrement le candidat sur la question de la correction des algorithmes proposés et sur la question de leur complexité, en temps comme en espace.

932 Fondement théorique des bases de données relationnelles.

932.1 Développements :

— 08 - L'inclusion de requêtes conjonctives est NP-Complet.

— 06 - Correction et complétude du système d'inférence d'Armstrong.

932.2 Rapport de Jury

Le cœur de cette nouvelle leçon concerne les fondements théoriques des bases de données relationnelles : présentation du modèle relationnel, approches logique et algébrique des langages de requêtes, liens entre ces deux approches.

Le candidat pourra ensuite orienter la leçon et proposer des développements dans des directions diverses : complexité de l'évaluation des requêtes, expressivité des langages de requête, requêtes récursives, contraintes d'intégrité, aspects concernant la conception et l'implémentation, optimisation de requêtes...

932.3 Programme

— Modèle relationnel

— Algèbre relationnelle

— Calcul relationnel

— théorème de Codd

— Calcul conjonctif

932.4 Réferences

— [AHV96]

— [Ull82]

CHAPITRE 9

BIBLIOGRAPHIE

[AHV96] S. Abiteboul, R. Hull, and V. Vianu. *Foundations of databases*. 1996.

[ASU86] A. V. Aho, R. Sethi, and J. D. Ullman. *Compiler : Principles, Techniques, and Tools*. 1986.

[Ave97] A. Avez. *Calcul différentiel*. 1997.

[BBC92] D. Beauquier, J. Berstel, and P. Chrétienne. *Éléments d'algorithmique*. 1992.

[Ber90] M. Berger. *Géométrie I*. 1990.

[Ber17] F. Berthelin. *Équations différentielles*. 2017.

[Ber18] L Bernis, J et Bernis. *Analyse pour l'agrégation de mathématiques, 40 développements*. 2018.

[BMP05] V. Beck, J. Malick, and G. Peyré. *Objectif agrégation*. 2005.

[Bré87] H. Brézis. *Analyse fonctionelle*. 1987.

[Car14] O. Carton. *Langages formels, calculabilité et complexité*. 2014.

[CG13] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries tome 1*. 2013.

[CG17a] P. Caldero and J. Germoni. *Nouvelles Histoires hédonistes de groupes et de géométries tome 1*. 2017.

[CG17b] P. Caldero and J. Germoni. *Nouvelles Histoires hédonistes de groupes et de géométries tome 2*. 2017.

[CHL07] M. Crochemore, C. Hancart, and T. Lecroq. *Algorithms on strings*. 2007.

[CL03] R. Cori and D. Lascar. *Logique Mathématique : Fonctions récursives, théorème de Gödel, théorie des ensembles, théorie des modèles*. 2003.

[CL05] A. Chambert-Loir. *Algèbre Corporelle*. 2005.

[CL06] P. G. Ciarlet and J.-L. Lions. *Introduction à l'analyse numérique matricielle et à l'optimisation*. 2006.

[CLF95] A. Chambert-Loir and S. Fermigier. *Exercices de Mathématiques pour l'agrégation, Analyse 2*. 1995.

[CLRS02] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein. *Introduction à l'algorithmique, 2eme édition*. 2002.

[Dem97] M. Demazure. *Cours d'algèbre*. 1997.

[DGH10] A. Durand-Gasselin and P. Habermehl. On the Use of Non-deterministic Automata for Presburger Arithmetic. In *Gastin P., Laroussinie F. (eds) CONCUR 2010 - Concurrency Theory. CONCUR 2010. Lecture Notes in Computer Science, vol 6269. Springer, Berlin, Heidelberg*, 2010.

[DM85] H. Dym and H. P. McKean. *Fourier Series and Integrals*. 1985.

[DNR03] R. David, K. Nour, and C. Raffalli. *Introduction à la logique*. 2003.

[Dow10] G. Dowek. *Les démonstrations et les algorithmes - Introduction à la logique et à la calculabilité*. 2010.

[FN07a] H. Francinou, S. Gianella and S. Nicolas. *Exercices de mathématiques Oraux de l'ENS : Algèbre 1*. 2007.

[FN07b] H. Francinou, S. Gianella and S. Nicolas. *Exercices de mathématiques Oraux de l'ENS : Analyse 1*. 2007.

[FN07c] H. Francinou, S. Gianella and S. Nicolas. *Exercices de mathématiques Oraux de l'ENS : Analyse 2*. 2007.

[GAA+13] Georges Gonthier, Andrea Asperti, Jeremy Avigad, Yves Bertot, Cyril Cohen, François Garillot, Stéphane Le Roux, Assia Mahboubi, Russell O'Connor, Sidi Ould Biha, Ioana Pasca, Laurence Rideau, Alexey Solovyev, Enrico Tassi, and Laurent Théry. A Machine-Checked Proof of the Odd Order Theorem. In *ITP 2013, 4th Conference on Interactive Theorem Proving*, 2013.

[GLM97] J. Goubault-Larrecq and I. Mackie. *Proof Theory and Automated Deduction*. 1997.

[Gou09] X. Gourdon. *Les maths en tête - Algèbre (2ème édition)*. 2009.

[Hin00] M. Hindry. *Arithmétique*. 2000.

[Laf97] J. Lafontaine. *Introduction aux variétés différentielles*. 1997.

[LM06] Y. Lacroix and L. Mazliak. *Probabilités : Variables aléatoires - Convergences - Conditionnement*. 2006.

[MM12] R. Mansuy and R. Mneimné. *Réduction des endomorphismes*. 2012.

[Mne86] F. Mneimné, R. et Testard. *Introduction à la théorie des groupes de Lie classiques*. 1986.

[Pap94] C. H. Papadimitriou. *Computational Complexity*. 1994.

[Per95] D. Perrin. *Cours d'algèbre*. 1995.

[Per14] S. Perifel. *Complexité Algorithmique*. 2014.

[Ran05] B. Randé. Un algorithme pour la décomposition en espaces cycliques. In *Revue de Mathématiques Spéciales RMS 115-4* , Mai 2005.

[Rom99] J.-E. Rombaldi. *Analyse Matricielle*. 1999.

[Rom17] J.-E. Rombaldi. *Mathématiques pour l'agrégation : algèbre et géométrie*. 2017.

[Rou03] F. Rouvière. *Petit guide de calcul differentiel à l'usage de la licence et de l'agrégation*. 2003.

[Ser02] D. Serre. *Matrices Theory and Applications*. 2002.

[SPR02] P. Saux Picart and É. Rannou. *Cours de calcul formel*. 2002.

[Ull82] Jeffrey D. Ullman. *Principles of Database Systems*. 1982.

[Win93] G. Winskel. *The Formal Semantics of Programming Languages*. 1993.

[ZQ13] C. Zuily and H. Queffélec. *Analyse pour l'agrégation - 4e éd.* 2013.