République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université de BATNA

Faculté des Sciences

Département de Mathématiques

MEMOIRE DE MAGISTER

Présenté Pour l'Obtention du Diplôme de Magister en Mathématiques

Option: *Analyse Fonctionnelle*

Thème:

Transformation De Fourier Discrète Et Applications

Présentée Par: MOKRANI IBTISSAM

Soutenu publiquement le: 20/01/2014

Devant le jury composé de:

Mr. BENAISSA Abdellah	***M C A (U. de Batna)***	***Président***
Mr. NOUI Lemnouar	***Professeur (U. de Batna)***	***Rapporteur***
Mr. DJEFFAL Lakhdar	***M C A (U. de Batna)***	***Examinateur***
Mr. KADEM Abdelwahab	***Professeur (U.de Setif)***	***Examinateur***

Dédicaces

Dédicaces

Je dédie ce modeste travail à :

A ma mère, Dieu ait son âme.

A mon père, que Dieu le protège.

A mon mari pour son soutien.

A Mes frères.

A Mes sœurs.

Et

A tous ceux qui me sont chers.

MOKRANI IBTISSAM

Remerciement

Remerciement

Je remercie Dieu tout puissant de m'avoir accorder la volonté et le courage pour réaliser ma thèse.

J'exprime ma profonde reconnaissance et mes vifs remerciements à ***Mr.NOUI Lemnouar****, Professeur au département de mathématiques à l'Université de Batna, pour m'avoir guidée et permis de terminer cette thèse.*

Un grand merci à ***Mr. BENAISSA Abdellah****, Maître de conférences à l'Université de Batna, pour avoir accepté de présider ce Jury.*

Mes remerciements les plus élogieux à ***Mr. DJEFFAL Lakhdar****, Maître de conférences au département de mathématiques à l'Université de Batna, et à* ***Mr. KADEM Abdelwahab****, Professeur à l'Université de Setif, de m'avoir honoré par leur présence au jury autant qu'examinateurs.*

Je vous remercie :

Mon père, que Dieu le protège.

Mon mari pour son soutien.

Mes frères et mes sœurs, merci pour vos encouragements, avec une pensée particulière à ma grand-mère et ma tante.

A tous ceux qui m'ont enseigné, je vous suis très reconnaissant.

A plusieurs proches, et mes amis, qui ont contribuées de près ou de loin à l'élaboration de ce travail, je ne serais les nommer toutes, mais je tiens à leurs exprimer mes vives remerciements.

MOKRANI IBTISSAM

TABLE DES MATIERES

TABLE DES MATIERES

Chapitre 5 : Variantes de la Transformée de Fourier

Introduction

Introduction

La transformée de Fourier et l'analyse fréquentielle ou spectrale, sont des outils fondamentaux pour la compréhension et la mise en œuvre de nombreuses techniques numériques de traitement des signaux et des images. On la trouve dans des domaines très variés.

On peut citer toutes les applications où il est nécessaire de mettre en forme les signaux mesurés par des capteurs grâce à un filtrage.

On l'utilise par exemple dans le codage à débit réduit de la parole, la reconnaissance vocale, l'amélioration de la qualité des images,la compression, les transmissions numériques, les nouveaux systèmes de radiodiffusion, dans les applications biomédicales (scanner, imagerie par résonance magnétique nucléaire), en astronomie (synthèse d'image par interférométrie), en modélisation de propagation d'ondes, en analyse spectrale pour l'étude de structures moléculaires ainsi qu'en cristallographie. Son extension (calculs sur les corps finis) est utilisée dans la theorie des codes lineaires concernant les méthodes de correction d'erreurs en transmission numérique.

Elle intervient aussi dans les méthodes envisagées en informatique quantique pour la factorisation de nombres.

L'objectif de ce mémoire est l'étude de la transformée de fourrier discrète, notion utile en théorie et en applications.

Dans ce mémoire on rappelle les notions mathématiques nécessaires pour aborder ce genre de question.

Le premier chapitre est consacré aux groupes, groupes cycliques (en particulier le groupe des racines nième de l'unité), décomposition des groupes abéliens finis.

Dans le deuxième chapitre, on a introduit les matrices circulantes et leur diagonalisation, outils indispensables pour définir la transformée de fourrier discrète, ensuite on a définit le produit de convolution discret et les matrices de Toeplitz .

Au troisième chapitre les caractères d'un groupe fini sont étudiés afin de généraliser la transformée fourrier à un groupe quelconque, ce qui fait l'objet du quatrième chapitre.

Le dernier chapitre est consacré aux variantes de la transformée de fourrier suivant le groupe de base, la transformée de fourrier sur le groupe cyclique $\frac{\mathbb{Z}}{n\mathbb{Z}}$, la transformée d'Hadamard sur $G = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^m$; et plus généralement sur $(\frac{Z}{nZ})^m$.

On termine par la transformée de fourrier sur les corps finis et on donne quelques exemples d'application à savoir le calcul du produit de deux polynômes et le produit de deux entiers.

Chapitre 1 :
Notions préliminaires sur les groupes

Chapitre 1

1-Notions préliminaires sur les groupes .

Définitions :

1-1 Groupe :

Soit G un ensemble non vide muni d'une loin interne .

$$G \times G \rightarrow G$$

$$(x,y) \rightarrow x.y$$

on dit que $(G,.)$ est un groupe si :

1) $(.)$ est un associative.
2) il existe un élément neutre 1 : $\forall x \in G : x.1 = 1.x = x$
3) tout élément $x \in G$ admet un inverse x^{-1} : $x.x^{-1} = x^{-1}.x = 1$.

Si de plus la loi $(.)$ est commutative : $xy = yx$ pour tout $x,y \in G$, On dit que G est un group commutatif .

Exemple :

1) $(\mathbb{Z},+)$ est un groupe infini .
2) $\frac{\mathbb{Z}}{n\mathbb{Z}}$ est un groupe commutatif fini pour le loi : $(+)$

$$\bar{x} + \bar{y} = \overline{x+y}$$

3) $(\mathbb{C},.)$ est un groupe commutatif multiplicatif infini .
4) $(\mathbb{Z};\times)$ n'est pas un groupe, $(\mathbb{R}[X];\times)$ non plus.
5) $(\{-1;1\};\times)$ est un groupe.
6) L'ensemble $\mathcal{F}(\mathbb{R};\mathbb{R})$ des applications de $\mathbb{R}$ dans $\mathbb{R}$ muni de la loi $+$ est un groupe dont l'élément neutre est la fonction nulle.
7) $((\frac{\mathbb{Z}}{n\mathbb{Z}})^*;\times)$ est un groupe dont l'élément neutre est $\bar{1}$.

Proposition :

Soit $(G;.)$ un groupe alors on a les propriétés suivantes :
1. L'élément neutre est unique.
2. Tout élément de x a un symétrique unique.

Démonstration :

Suposons qu'il existe e_1 et e_2 deux éléments neutres de G, alors
$e_1\ e_2 = e_1$ car e_2 est un élément neutre
$e_1\ e_2 = e_2$ car e_1 est un élément neutre
donc $e_1 = e_2$.
Supposons qu'il existe un élément x ayant deux symétriques x_1 et x_2 donc $xx_1 = e$ et $x_2\ x = e$ alors

$$x_2.(x.x_1) = x_2.e = x_2$$

mais par associativité de . on a

$$x_2.(x.x_1) = (x_2.x).x_1 = e.x_1 = x_1$$

et donc

$$x_1 = x_2$$

1-2 Sous - groupe :

Soit H une partie non vide du groupe $(G,.)$
H est un sous - groupe de G si:

$$\forall x,y \in H\ ,\ x.y^{-1} \in H$$

Si le groupe G est additif , H est un sous - groupe de G si est seulement si $x,y \in H \Rightarrow x - y \in H$.

Exemple :

1 - nZ est un sous groupe de $(Z,+)$.
2- L'ensemble des nombres pairs est un sous groupe de $(\mathbb{Z};+)$; mais pas l'ensemble des nombres impairs.
3- $\mathbb{Z}[X]$: polynômes à coefficients dans $\mathbb{Z}$ est un sous-groupe de$(\mathbb{R}[X];+)$.
4- Soit $\vec{u}$ un vecteur (du plan ou de l'espace) alors l'ensemble des vecteurs colinéaires à $\vec{u}$:

$$\left\{\vec{v} \text{ tel que } \exists k \in \mathbb{Z}; \vec{v} = k\vec{u}\right\}$$

est un sous-groupe du groupe des vecteurs (du plan ou de l'espace) muni de l'addition .

1-3 Ordre d'un élément et groupe cyclique .

On va maintenant donner quelques définitions .

* Ordre d'un élément :

Définition :

Soit $(G;.)$ un groupe, et soit $g \in G$, on note $\langle g \rangle$ le sous-groupe engendré par g; donc $\langle g \rangle = \{g^{-2}; g^{-1}; 1; g; g^2; \ldots; \}$

Proposition :

Si $(G;.)$ est un groupe fini, pour tout $g \in G$ il existe un entier positif k minimal tel que $g^k = 1$ et alors $\langle g \rangle = \{1; g; g^2; \ldots; g^{k-1}\}$

k s'appelle l'ordre de g et est noté $ord(g)$. On a de plus $ord(g) = card\ \langle g \rangle$

Démonstration :

Si G est fini, $\langle g \rangle$ est fini donc il existe a et $b \in \mathbb{Z}$ tel que $g^a = g^b$ donc $g^{|a-b|} = 1$ donc

$\{x \in \mathbb{N}, g^x = 1\}$ est non vide donc il admet un élément minimal : k.

On a évidemment $\{1; g; g^2; \ldots; g^{k-1}\} \subset \langle g \rangle$, réciproquement soit $\langle g \rangle$ un élément de g^x, effectuons la division euclidienne de $x$par k,

on obtient $x = kd + r$ où $0 \leq r < k$ et donc $g^k = g^{kd+r} = (g^k)^d g^r = g^r$

donc $g^k \in \{1; g; g^2; \ldots; g^{k-1}\}$.

Il reste à montrer que card $card\ \langle g \rangle = k$ et donc que tous les éléments de $\{1; g; g^2; \ldots; g^{k-1}\}$ sont distincts, mais si on avait $g^x = g^y$avec $0 \leq x < y \leq k-1$alors on aurait $g^{y-x} = 1$ où $0 < y - x \leq k - 1$

or ceci est impossible par définition de k.

** Groupe cyclique :

Définition :

Soit $(G;.)$ un groupe fini, G est dit cyclique si il existe un élément g de G tel que $G = \langle g \rangle$. On dit que g est un générateur de G.

Exemple :

Le groupe $(\frac{\mathbb{Z}}{n\mathbb{Z}};+)$ est cyclique, en effet $\frac{\mathbb{Z}}{n\mathbb{Z}} = \langle 1\rangle$.

Il faut remarquer que dans un groupe cyclique tous les éléments ne sont pas des générateurs par exemple dans $\frac{\mathbb{Z}}{10\mathbb{Z}}$, $\langle 5\rangle = \{0;5\}$ et $\langle 2\rangle = \{0;2;4;6;8\}$ alors que $\langle 3\rangle = \langle 7\rangle = \frac{\mathbb{Z}}{10\mathbb{Z}}$.

On va maintenant donner le nombre de générateurs d'un groupe cyclique.

Proposition :

Soit $(G;.)$ un groupe cyclique de cardinal n. Le nombre de générateurs de G est $\varphi(n)$.

Démonstration :

Soit g un générateur de G et soit h un élément de G il existe donc un entier positif $k \leq n-1$

tel que $h = g^k$, on va montrer que

$$G = \langle k\rangle \Leftrightarrow k \wedge n = 1$$

ce qui donnera le résultat puisque $\varphi(n)$ est le nombre d'entiers positifs inférieurs à n qui sont premiers avec n

Si $k \wedge n = 1$ d'après le théorème de Bézout, il existe deux entiers u et v tels que $ku + nv = 1$

donc $g = g^{ku+nv} = h^u 1^v = h^u$, par conséquent pour tout entier d on a $h^{ud} = g^d$ et donc $G = \langle h\rangle$.

Réciproquement :

si $G = \langle h\rangle$ alors il existe un entier u tel que $h^u = g$ donc $g^{ku-1} = 1$ donc $ku-1$ est multiple de$n$ donc il existe un entier r tel que $ku - 1 = rn$ et on a donc $ku - rn = 1$ et donc d'après le théorème de Bézout $k \wedge n = 1$.

Exemple :

a) $\frac{Z}{5Z} = \left\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\right\}$ est un groupe cyclique engendré par $\bar{1}$: $1\,\bar{1},\ 2\,\bar{1},\ 3\,\bar{1},\ 4\,\bar{1},\ 5\,\bar{1} = 0$.

b) $(\frac{Z}{5Z})^* = \frac{Z}{5Z} - \{0\} = \left\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4}\right\}$ est un groupe cyclique engendré par $(\bar{2})$

$$\left(\frac{Z}{5Z}\right)^* = \langle\bar{2}\rangle = \{2^1, 2^2 = 4, 2^3 = 3, 2^4 = 1\}$$

Groupe des racines n = ieme de l'unité

$$U_n = \{z \in \mathbb{C} / z^n = 1\} = \{e^{\frac{2ik\pi}{n}}, 0 \leq k \leq n-1\}$$

est un groupe cyclique engendré par $e^{\frac{2ik\pi}{n}}$.

$$z \in U_n \Rightarrow z = \left(e^{\frac{2ik\pi}{n}}\right)^k$$

on montre que les générateurs de U_n sont de la forme $e^{\frac{2ik\pi}{n}}$ avec k et n premiers entre eux .

d'une façon générale si $G = \langle x \rangle$, x^k est un générateur de $(G,.)$ si est selement si k est premier avec n l'ordre de $G[.]$.

le nombre de ses générateurs est calculé par la fonction d'euler :
$\varphi(n) = card\ \{k / 0 \leq k \leq n\ , \triangle(k,n) = 1\}$.

si $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_{\triangle}^{\alpha_{\triangle}}$ est décomposé en produit de facteurs premiers , $\varphi(n)$ est calculé par :

$$\varphi(n) = n\ (1 - \frac{1}{p_1})(1 - \frac{1}{p2}) \ldots . (1 - \frac{1}{p\triangle}).$$

en particulier si $n = p^k$ premier :

$$\varphi(n) = p^k - p^{k-1}$$

Exemple :

a) $G = \frac{Z}{5Z}$ on a $\varphi(5) = 5 - 1 = 4$ générateurs .
b) $G = \frac{Z}{4Z}$ on a $\varphi(4) = 2^2 - 2^1 = 2$ générateurs .

1-4Théorème de lagrange :

Soit $(G;.)$ un groupe fini, soit H un sous-groupe de G alors le cardinal de H divise le cardinal de G.

Démonstration :

Soit la relation binaire $\Re$ définie sur G par :

$$x \Re y \Leftrightarrow xy^{-1} \in H\ ,\ \forall (x,y) \in G^2$$

a. Montrons que $\Re$ est une relation d'équivalence :

$xx^{-1} = 1 \in H \Leftrightarrow x \Re x$, donc $\Re$ est réflexive.

$x \Re y \Leftrightarrow xy^{-1} \in H$ (H sous groupe) $\Leftrightarrow (xy^{-1})^{-1} \in H \Leftrightarrow yx^{-1} \in H \Leftrightarrow y \Re x$, donc $\Re$ est symétrique.

$(x \Re y$ et $y \Re z) \Rightarrow (xy^{-1} \in H$ et $yz^{-1} \in H) \Rightarrow (xy^{-1}yz^{-1} = xz^{-1} \in H) \Rightarrow x \Re z$, donc $\Re$ est transitive.

Donc $\Re$ est bien une relation d'équivalence.

La classe d'équivalence d'un élément a de G est, par définition :

$$\{y \in G / a \Re y\} = \{y \in G / a^{-1}y \in H\} = \{y \in G / \exists h \in H, a^{-1}y = h\}$$

$$= \{y \in G / \exists h \in H, a^{-1}y = ah\}$$

$$= aH$$

Cet ensemble est appelé classe à gauche (de a) modulo H.

b. Montrons que toutes les classes à gauche ont $|H|$ éléments :

Pour cela, on considère, pour tout $a \in G$, l'application

$$f_a : H \to aH$$

$$h \to ah$$

- $f_a(h_1) = f_a(h_2) \Rightarrow ah_1 = ah_2 \Rightarrow h_1 = h_2$, donc f_a est injective.
- $\forall y \in aH$, $\exists h \in H$ tel que $y = ah$, donc f_a est surjective.

f_a étant bijective, on déduit :

$$\forall a \in G \ |aH| = |H|$$

c. Montrons que toutes les classes à gauche sont disjointes :

Considérons deux classes aH et bH ($(a ; b) \in G^2$)
Et supposons

$$aH \cap bH \neq \emptyset$$

Soit $g \in aH \cap bH$. Alors :

$\exists h \in H$ tel que $g = ah$ et $\exists h' \in H$ tel que $g = ah'$

On à alors :

$$ah = ah'$$

$$a = bh'h^{-1}$$

Tout élément $ah"$ de aH s'écrit donc :

$$bh'h^{-1}h''$$

Or, $h'h^{-1}h'' \in H$, donc tout élément $ah"$ de aH est aussi élément de bH, d'où :

$$aH \subset bH$$

On montre, de même :

$$bH \subset bH$$

On a donc :

$$bH = bH$$

Ceci prouve que les classes à gauches sont disjointes.

Et enfin

En notant m le nombre de classes à gauches, on a donc :

$$G = \cup_{n=1}^{m} a_n H$$

D'où :

$$|G| = \sum_{n=1}^{m} |a_n H| = \sum_{n=1}^{m} |H| = m|H|$$

Alors

L'ordre du sous-groupe H divise donc l'ordre du groupe G.

1-5 Homomorphismes :

Soit $(G_1, .)$ et $(G_2, .)$ deux groupes et f une application de G_1 dans G_2 , on dit que f est un homomorphisme si $f(ab) = f(a)f(b)$ pour tout $a, b \in G_1$.

le noyau de f est défini par : $f^{-1}(G_2) = \{x \in G_1 / f(x) = 1\}$.

et image de f est définie par : $\mathrm{Im} f = \{y \in G_2 / y = f(x), x \in G_1\}$.

si f est bijective on dit que f est un isomorphisme de groupes .

Exemple :

1) Soit $n_0 \in \mathbb{Z}$. L'application $f : \mathbb{Z} \to \mathbb{Z}$ donnée par $\forall m \in \mathbb{Z}\ f(m) = n_0 m$ est un morphisme de groupes.

2) Soit $(G, .)$ un groupe, soit $a \in G$. Alors l'application $f : (\mathbb{Z}, +) \to (G, .)$ définie par :

$\forall n \in \mathbb{Z} f(n) = a^n$ est un morphisme de groupes.

3) L'application canonique $\mathbb{Z} \to \frac{\mathbb{Z}}{n\mathbb{Z}}$ qui à chaque élément x de $\mathbb{Z}$ associe sa classe modulo x est un morphisme de groupes.

4) On note $GL(n, \mathbb{R})$ le groupe des matricces inversibles $n \times n$ à coefficients dans $\mathbb{R}$.

Alors l'application $GL(n, \mathbb{R}) \to (\mathbb{R}\backslash\{0\}, \times)$ qui à tout M associe son déterminant est un morphisme de groupes.

1-6 Groupe quotient :

Comme les groupes utilisés par la suite sont commutatifs , on définit le quotient dans le cas d'un groupe commutatif G .

$\frac{G}{H} = \{x+H, x \in G\}$ (appelé ensemble des classes , $\bar{x} = x+H$).

cet ensemble est muni d'une structure de groupe par la loi

$$\bar{x} + \bar{y} = \overline{x+y}$$

(et on montre que la loi est bien définie , c'est à dire le résultat obtenu ne depend pas du choix des représentants des classes $\bar{x}$, $\bar{y}$).

ce groupe ainsi obtenu est dit groupe quotient de G par H .

Exemple:

$G = \mathbb{Z}$, $H = 3\mathbb{Z}$ on a

$$\frac{G}{H} = \frac{G}{3\mathbb{Z}} = \{\bar{0}, \bar{1}, \bar{2}\}$$

1-7 Décomposition des groupes abéliens finis :[1] , [2]

Théorème :

Tout groupe abélien fini G est prouduit d'un nombre fini de groupes cycliques , c'est à dire

$$G = \prod_{i=1}^{m} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$$

Théorème chinois :

Soient m et n deux nombres premiers entre eux alors le groupe $\frac{\mathbb{Z}}{mn\mathbb{Z}}$ est isomorphe à $\frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$.

Démonstration :

Soient a et b deux entiers premiers entre eux. Si x désigne un entier, on notera $cl_a(x)$ la classe de x modulo a, $cl_b(x)$ la classe de x modulo b.

et $cl_N(x)$ la classe de x modulo $N = ab$. Soit f l'application définie sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$, à valeurs dans $(\frac{\mathbb{Z}}{a\mathbb{Z}}) \times (\frac{\mathbb{Z}}{b\mathbb{Z}})$ définie par $cl_N(x) \mapsto (cl_a(x); cl_b(x))$.

Vérifions que f est bien définie.

Soient x et y tels que $cl_N(x) = cl_N(y)$. N divise $x-y$, c'est- à-dire ab divise $x-y$. Par suite, a divise $x-y$ et b divise $x-y$.

On a donc $cl_a(x) = cl_a(y)$ et $cl_b(x) = cl_b(y)$ et donc

$$f(cl_N(x)) = f(cl_N(y))$$

Montrons maintenant que f est linéaire. Soient $x; y \in \mathbb{Z}$.

$f(cl_N(x) + cl_N(y)) = f(cl_N(x+y))$ (définition de l'addition dans $\frac{\mathbb{Z}}{N\mathbb{Z}}$)

$$= (cl_a(x+y); cl_b(x+y))$$

(définition de la fonction f)

$$= (cl_a(x) + cl_a(y); cl_b(x) + cl_b(y))$$

(définition de l'addition dans $\frac{\mathbb{Z}}{a\mathbb{Z}}$ et $\frac{\mathbb{Z}}{b\mathbb{Z}}$)

$$= (cl_a(x); cl_b(x)) + (cl_a(y); cl_b(y))$$

(définition de l'addition sur $\frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}$)

$$= f(cl_N(x)) + f(cl_N(y))$$

De même, on montre que

$$f(cl_N(x).cl_N(y)) = f(cl_N(x)).f(cl_N(y)).$$

De plus, $f(cl_N(1)) = (cl_a(1); cl_b(1))$ et $(cl_a(1); cl_b(1))$ est l'unite de $\frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}$.

f est donc un morphisme d'anneaux.

Montrons que f est injective. Soit $x \in \mathbb{Z}$ tel que

$$f(cl_N(x)) = (cl_a(0); cl_b(0))$$

Alors $cl_a(x) = cl_a(0)$ donc a divise x.

De même, $cl_b(x) = cl_b(0)$

donc b divise x. a et b etant premiers entre eux, il en résulte que ab divise x, c'est- à-dire $cl_N(x) = cl_N(0)$. f est donc injective.

Pour terminer,il reste à montrer que f est surjective.

Soit

$$(cl_a(\alpha); cl_b(\beta)) \in \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}$$

On cherche $x \in \mathbb{Z}$ tel que

$$f(cl_N(x)) = (cl_a(\alpha); cl_b(\beta))$$

c'est- à-dire x tel que $x \ (mod\ a)$ et $x \ (mod\ b)$.

D'après le théorème des restes chinois, on sait qu'un tel x existe. f est donc surjective.

Remarque :

Si m et n ne sont pas premiers entre eux l'isomorphisme cité ci-dessus est faux .

Exemple :

Résoudre dans $\mathbb{Z}$ le système suivant :

$$\begin{cases} x \equiv 4(\text{mod } 5) \\ x \equiv 3(\text{mod } 6) \\ x \equiv 2(\text{mod } 7) \end{cases}$$

$5 \wedge 6 \wedge 7 = 1$. On applique le théorème des restes chinois, avec $n_1 = 5$; $n_2 = 6$; $n_3 = 7$; $N = 210$; $a_1 = 4$; $a_2 = 3$

et $a_3 = 2$. On sait que ce système admet une unique solution modulo 210, donnée par $x = u_1 a_1 N_1 + u_2 a_2 N_2 + u_3 a_3 N_3$, où

$N_1 = \frac{N}{n_1} = \frac{210}{5} = 42$, $N_2 = \frac{N}{n_2} = \frac{210}{6} = 35$, $N_3 = \frac{N}{n_3} = \frac{210}{7} = 30$, et u_1; u_2; u_3 sont les inverses respectifs de N_1;N_2;N_3 modulo n_1; n_2; n_3.

$42 \wedge 5 = 1$. D'après le théorème de Bezout, il existe $(u;v) \in \mathbb{Z}^2$ tel que $42u + 5v = 1$. L'algorithme d'Euclide donne :

$$42 = 5 \times 8 + 2$$

$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

En remontant cet algorithme, on obtient successivement :

$$1 = 5 - 2 \times 2$$

$$1 = 5 - (42 - 5 \times 8) \times 2$$

$$1 = 5 - 42 \times 2 + 5 \times 16$$

$$42(-2) + 5 \times 17 = 1$$

On en déduit que

$$u_1 = -2$$

Un raisonnement analogue conduit à $u_2 = -1$ et $u_3 = -3$.

Par suite, $x \equiv -2 \times 4 \times 42 + (-1)3 \times 35 + (-3) \times 30 \times 2(mod\ 210)$, c'est- à-dire $x \equiv 9(mod\ \ 210)$ (aprés simplifications).

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \neq \frac{\mathbb{Z}}{4\mathbb{Z}}$$

en effet $\frac{\mathbb{Z}}{4\mathbb{Z}}$ est cyclique mais $\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ ne l'est pas .

dans le théorème (1) si on choisit la suite $(n_1,\ldots,n_m)$ de telle sorte que n_{i+1} divise n_i pour tout i entier entre 1 et $m-1$ alors

la suite $(n_1,\ldots,n_m)$ est unique , ses élèment son dits facteurs invariants .

Exemple :

Un groupe d'ordre 96 : $G = \frac{\mathbb{Z}}{12\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$ admet pour facteurs invariants : $12,4,2$ un groupe cyclique d'rdre 96 : $G = \frac{\mathbb{Z}}{96\mathbb{Z}}$, ses facteurs sont 96 .

1-8 Indexation des élèments d'un groupe abélien fini:[1],[2]

On distingue trois cas :

Premier cas :

G est cyclique.
G est isomorphe à $(\frac{\mathbb{Z}}{n\mathbb{Z}},+)$, ses élèments sont présentés par $\{0,1,\ldots,n-1\}$

Exemple :

$G = \frac{\mathbb{Z}}{4\mathbb{Z}}$ est cyclique, ses élèment sont : $\{0,1,2,3\}$.

Deuxième cas :

$$G = (\frac{\mathbb{Z}}{2\mathbb{Z}})^m$$

dans ce cas on utilise l'écriture binaire des entiers compris 0 et $2^m - 1$, d'une façon précise tout élèment $(u_1, u_{2;}\ldots, u_m)$ de G et indexé par l'entier

$$u = u_1 2^0 + u_2 2^1 + \ldots + u_m 2^{m-1} = \sum_{i=1}^{m} u_i 2^{i-1}$$

Exemple :

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}}$$

donc on a

$$(0,0),(0,1),(1,0),(1,1)$$

alors par exemple

$$(u_1, u_2) = (1,1) = u_1 2^0 + u_2 2^1$$

$$= 1 \times 1 + 1 \times 2$$

$$= 3$$

Cas général :

Posons $e_1 = 1$ et on définit e_i pour $i \succ 1$ par

$$e_i = \Pi n_j, 1 \leq j \leq i$$

alors tout élèment est représenté par l'entier

$$u = \sum_{i=1}^{m} u_i e_i$$

Exemple :

$$\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{4\mathbb{Z}}$$

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

$$e_1 = 1, e_2 = \Pi_{1 \leq j \leq 2} n_j = n_1 \times n_2 = 8$$

alors par exemple $(u_1, u_2) \rightarrow u = u_1 e_2 + u_2 e_1$, donc

$$(0,0) \rightarrow 0$$

$$(0,1) \rightarrow 0 \cdot 1 + 1 \cdot 8 = 8$$

$$(0,2) \rightarrow 16$$

$$(0,3) \rightarrow 24$$

$$(1,0) \rightarrow 1$$

$$(1,1) \rightarrow 9$$

$$(1,2) \rightarrow 17$$

$$(1,3) \rightarrow 25$$

Chapitre 2 :
Les matrices circulantes

Chapitre 2

2-Les matrices circulantes .

2-1 Définition :

La matrice $C = (c_{i;j})$ de taille $n \times n$ est dite circulante si elle est de la forme suivante :

$$C = \begin{pmatrix} c_0 & c_1 & c_2 & \dots & c_{n-1} \\ c_{n-1} & c_0 & c_1 & \dots & c_{n-2} \\ c_{n-2} & c_{n-1} & c_0 & \dots & c_{n-3} \\ . & . & . & . & . \\ . & . & . & . & . \\ c_1 & c_2 & c_3 & \dots & c_0 \end{pmatrix}$$

où les coefficients $c_{i;j}$; $i;j \in \{0, n-1\}$ sont des éléments d'un corps K , telle que chaque ligne se déduit de la ligne précédente par une permutation circulaire .

Exemple :

$$C = \begin{pmatrix} -1 & i & \sqrt{3} \\ \sqrt{3} & -1 & i \\ i & \sqrt{3} & -1 \end{pmatrix}$$

est une matrice circulante d'ordre 3.

2- 2Algèbre des matrices circulantes :

2-2-1 Définition d'une algèbre :

En mathématiques ,une algèbre sur un corps commutatif K ou simplement une K-algèbre est une structure algèbrique $(A, +, ., \times)$ telle que :

$(A, +, .)$ est un espace vectoriel sur K.

La loi $\times$ est définie de $A \times A$ dans A (loi de composition interne).

La loi $\times$ est distributive par rapport à la loi $+$

Pour tout (a,b) dans K^2 et pour tout (x,y) dans A^2.

$$(a.x) \times (b.y) = (ab).(x \times y)$$

Pour alléger les notations , on désigne par C ($c_0, c_1, \ldots, c_{n-1}$) la matrice circulante précédente (engendrée par la première ligne $c_0, \ldots, c_{n-1}$).

En notant $J = C(0,1,0,\ldots\ldots,0)$, On peut constater que toute matrice circulante est un polynôme en J : C ($c_0, c_1, \ldots, c_{n-1}$) = $c_0 I_n + c_1 J + \cdots\cdots + c_{n-1} J^{n-1}$.

Exemple :

$$C(-1, i, \sqrt{3}\ ) = \sum_{j=0}^{2} c_j J^j$$

$$= c_0 J^0 + c_1 J^1 + c_2 J^2$$

$$J^0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}; J^1 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} :$$

$$J^2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

Donc

$$C(-1, i, \sqrt{3}\ ) = -1\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} + i\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} + \sqrt{3}\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$= \begin{pmatrix} -1 & i & \sqrt{3} \\ \sqrt{3} & -1 & i \\ i & \sqrt{3} & -1 \end{pmatrix}$$

$$= C$$

2-2-2 Diagonalisation de J :

L' ensembles des matrices circulantes est une algébre pour l àddition et le produit des matrices et la multiplication par un scalaire.

La matrice J vérifiant $J^n = I$, elle est diagonalisable sur $\mathbb{C}$.

Les valeurs propres sont des racines n-èmes de l'unité; elles forment un groupe cyclique pour le produit .

On prend donc $\omega = e^{\frac{2i\pi}{n}}$, une racine primitive de l'unité qui est un générateur du groupe cyclique en question .

En effet ; soit X un vecteur propre associé à la valeur propre λ de J :
On à : $JX = \lambda X$ alors

$$J^2X = J(\lambda X) = \lambda^2 X$$

et

$$J^3 X = \lambda^3 X$$

$$\vdots$$

d'une facon générale

$$J^m X = \lambda^m X$$

Alors pour $m = n$ on obtient

$$X(1 - \lambda^n) = 0 \quad (X \neq 0)$$

donc $\lambda^n = 1$et λ est une racine n-èmes de l'unité.
Comme les valeur propres $\lambda_i = e^{\frac{2i\pi k}{n}}$ avec $k = 0;\ldots;n-1$ sont distinctes alors J est diagonalisable sur $\mathbb{C}$.

Exemple :

Considérons la matrice

$$J = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Cette matrice admet comme valeur propres

$$\lambda_0 = 1 \ : \quad \lambda_1 = \frac{-1 + i\sqrt{3}}{2} \ : \ \lambda_2 = \frac{-1 - i\sqrt{3}}{2} \ :$$

Ou encore

$$\lambda_i \in \{\, 1,\ e^{\frac{2i\pi}{3}} \ ,\ e^{\frac{-2i\pi}{3}} \,\}$$

Les racines primitives troisièmes de l'unité sont :

$$\{\, \frac{-1 + i\sqrt{3}}{2} \ , \frac{-1 - i\sqrt{3}}{2} \,\}$$

Ainsi J qui est de taille 3×3 a trois valeurs propres distinctes ,donc elle est diagonalisable sur $\mathbb{C}$.
Si nous voulons diagonaliser J ; nous avons besoin de déterminer les vecteurs propres correspondonts , par exemple ,
On a :

$$J X_0 = \lambda_0 X_0$$

Alors

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

Alors

$$\begin{cases} x_2 = x_1 \\ x_3 = x_2 \\ x_1 = x_3 \end{cases}$$

donc

$$X_0 = x_3 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

et posons

$$V_0 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$$

$$J X_1 = \lambda_1 X_1$$

alors

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = e^{\frac{2i\pi}{3}} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

.

et

$$\begin{cases} x_2 = e^{\frac{2i\pi}{3}} x_1 \\ x_3 = e^{\frac{2i\pi}{3}} x_2 \\ x_1 = e^{\frac{2i\pi}{3}} x_3 \end{cases}$$

et

$$X_1 = x_3 \begin{pmatrix} \lambda_1 \\ \lambda_1^2 \\ \lambda_1^3 \end{pmatrix}$$

posons

$$V_1 = \begin{pmatrix} \lambda_1 \\ \lambda_1^2 \\ \lambda_1^3 \end{pmatrix}$$

Et de même on obtient

$$X_2 = x_3 \begin{pmatrix} \lambda_2 \\ \lambda_2^2 \\ \lambda_2^3 \end{pmatrix}$$

posons

$$V_2 = \begin{pmatrix} \lambda_2 \\ \lambda_2^2 \\ \lambda_2^3 \end{pmatrix}$$

La matrice de passage pour la diagonalisation est

$$P = \begin{pmatrix} 1 & \lambda_1 & \lambda_2 \\ 1 & \lambda_1^2 & \lambda_2 \\ 1 & \lambda_1^3 & \lambda_2^3 \end{pmatrix}$$

On à

$$P^{-1}JP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{\frac{2i\pi}{3}} & 0 \\ 0 & 0 & e^{\frac{-2i\pi}{3}} \end{pmatrix} = \begin{pmatrix} \lambda_0 & 0 & 0 \\ 0 & \lambda_1 & 0 \\ 0 & 0 & \lambda_2 \end{pmatrix}$$

Pour le cas général on vérifie alors sans peine que pour tout entier k

$$V_k = \begin{pmatrix} 1 \\ \omega^k \\ \omega^{2k} \\ \vdots \\ \omega^{(n-1)k} \end{pmatrix}$$

est un vecteur propre associé à la valeur propre

$$\lambda_k = e^{\frac{2ik\pi}{n}} = \omega^k \qquad .K = 0, \ldots\ldots, n-1$$

Remarque :

On peut choisir la matrice de passage P formée des vecteurs propres de sorte à obtenir une base orthonormée.

2-2-3 La transformée du Fourrier discrète :

K est un corps fini ou infini.

A est une matrice circulante
ω est une racines n-èmes de l'unité
La transformée de Fourrier Discrète est une application définie par

$$TFD \quad : K^n \to K^n$$

$$X \mapsto f(X) = AX$$

où

$$A = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & \omega^{n-1} & \dots & \omega^{(n-1)^2} \end{pmatrix}$$

2–2-4 Diagonalisation d'une matrice circulante :

Rappelons la proposition suivante

Proposition :

Si A est une matrice de type $n \times n$; λ une de ses valeurs propres :

$$AX = \lambda X$$

et

$$P(X) = \quad a_0 + a_1 X + \cdots + a_m X^m$$

est un polynôme alors la matrice

$$P(A) = \quad a_0 I + a_1 A + \cdots + a_m A^m$$

a pour valeur propre

$$P(\lambda) = \quad a_0 + a_1 \lambda + \cdots + a_m \lambda^m$$

c'est à dire il existe un vecteur non nul X tel que

$$P(A)X = P(\lambda)X$$

Démonstration :

Premièrement nous montrous que si λ est une valeur propre de A et $p \in \mathbb{N}^*$ alors λ^p est une valeur propre de A^p.

Soient λ une valeur propre de A et V un vecteur propre associé a cette valeur, donc

$$AV = \lambda V$$

Donc il suffit de montrer l'égalite suivante :

$$A^pV = \lambda^pV \quad \forall p \in \mathbb{N}^*$$

par récurrence.

• $AV = \lambda V$ donc la propriété est vraie pour $p = 1$.

• Supposons la propriété vraie pour un certain rang n, c'est-à-dire supposons que

$$A^nV = \lambda^nV$$

Alors

$$A^{n+1}V = AA^nV = A\lambda^nV = \lambda^nAV = \lambda^n\lambda V = \lambda^{n+1}V$$

par conséquent

$$A^{n+1}V = \lambda^{n+1}V$$

La propriété est donc vraie au rang $n+1$.

d'ou elle est vraie quel que soit l'entier naturel p.

Donc si λ est une valeur propre de A associée au vecteur propre V ,alors λ^pest une valeur propre de A^p associée au même vecteur propre V et les vecteurs propres de A sont des vecteurs propres de A^p .

Comme

$$p(A)V = (a_0I + a_1A + \cdots + a_mA^m)V = a_0V + a_1AV + \cdots + a_mA^mV$$

$$= a_0V + a_1\lambda V + \cdots + a_m\lambda^mV$$

Donc, nous avons

$$p(A)V = p(\lambda)V$$

En conclusion si λ est une valeur propre de A associée au vecteur propre V ,alors $p(\lambda)$ est une valeur propre de $p(A)$ associée au même vecteur propre V et les vecteurs propres de A sont des vecteurs propres de $p(A)$.

Exemple :

Soient I_5 la matrice identite d'ordre 5 , A et B les matrices d'ordre 5 à coefficients complexes définies par

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{et} \quad B = \begin{pmatrix} a & e & d & c & b \\ b & a & e & d & c \\ c & b & a & e & d \\ d & c & b & a & e \\ e & d & c & b & a \end{pmatrix}$$

Premièrement prouvons qu'il existe un polynôme Q de $\mathbb{C}[X]$ tel que

$$B = Q(A)$$

On calcule

$$A^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$A^3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$$A^4 = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \times \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

donc

$$B = aI_5 + bA + cA^2 + dA^3 + e\,A^4$$

D'où $B = Q(A)$ avec

$$Q(X) = a + bX + cX^2 + dX^3 + e\,X^4$$

.

Donc par la proposition precedente on deduit que pour trouver les valeurs propres de B il suffit de calculer les valeurs propres de A

Pour cela , on calcule le polynôme caractéristique de$A$: $\det(A - XI_5)$.

On trouve :

$$p_{car,A}(X) = -(X^5 - 1)$$

donc les valeur propres de A sont :

$\lambda_0 = 1$, $\lambda_1 = e^{\frac{2i\pi}{5}}$, $\lambda_2 = e^{\frac{4i\pi}{5}}$, $\lambda_3 = e^{\frac{6i\pi}{5}}$, $\lambda_4 = e^{\frac{8i\pi}{5}}$, et comme la matrice A d'ordre 5 a cinq valeurs distinctes , donc A est diagonalisable ,et donc B est aussi diagonalisable et ses valeur propres sont :

$$Q(\lambda_0) \ , Q(\lambda_1) \ , Q(\lambda_2) \ , Q(\lambda_3) \ , Q(\lambda_4)$$

donc les valeur propres de B sont :

$$a+b+c+d+e \ , \quad a+be^{\frac{2i\pi}{5}}+ce^{\frac{4i\pi}{5}}+de^{\frac{6i\pi}{5}}+ee^{\frac{8i\pi}{5}} \ , \quad a+be^{\frac{4i\pi}{5}}+ce^{\frac{8i\pi}{5}}+de^{\frac{12i\pi}{5}}+e\,e^{\frac{16i\pi}{5}} \ ,$$

$$a+be^{\frac{6i\pi}{5}}+ce^{\frac{12i\pi}{5}}+de^{\frac{18i\pi}{5}}+e\,e^{\frac{24i\pi}{5}}, \quad a+be^{\frac{8i\pi}{5}}+ce^{\frac{16i\pi}{5}}+de^{\frac{24i\pi}{5}}+e\,e^{\frac{32i\pi}{5}}$$

Montrons maintenant que toute matrice circulaire $C(c_0, \dots, c_{n-1})$ est diagonalisable ?

Comme $C(c_0, \dots, c_{n-1}) = c_0 + c_1 J + \cdots + c_{n-1} J^{n-1} = P_c(J)$

avec

$$P_c(X) = c_0 + c_1 X + \cdots + c_{n-1} X^{n-1}$$

Comme J est diagonalisable : $JV_k = \lambda_k V_k$ alors

$$C(c_0, \dots, c_{n-1}) V_k = P_c(\lambda_k)\, V_k$$

donc $\lambda_k^{'} = P_c(\lambda_k) = P_c(\omega^k)$ sont les valeurs propres de C et V_k sont les vecteurs propres de C .

$(\lambda_i') = U.(c_i)$, où U est une matrice de Vandermonde de déterminant non nul car les valeurs λ_k sont distinctes; donc U est inversible , d'où

$(c_i) = U^{-1}(\lambda_i')$ et comme $U^* U = I$ alors :

$$U^{-1} = U^* = {}^t\overline{U}$$

Posons :

$$\frac{1}{\sqrt{n}} U = u$$

$$(\lambda_i') = U.(c_i)$$

alors

$$(c_i) = U^{-1}(\lambda_i')$$

et $(c_i) = \frac{1}{\sqrt{n}} u^{-1}(\lambda_i')$ et $(c_i) = \frac{1}{\sqrt{n}} \overline{u^t}(\lambda_i')$

$$\bar{u} = \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \varpi & \dots & \varpi^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & \varpi^{n-1} & \dots & \varpi^{(n-1)^2} \end{pmatrix}$$

$$(c_i) = \frac{1}{\sqrt{n}} \cdot \frac{1}{\sqrt{n}} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \varpi & \dots & \varpi^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & \varpi^{n-1} & \dots & \varpi^{(n-1)^2} \end{pmatrix} (\lambda_i')$$

$$= \frac{1}{n} \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \varpi & \dots & \varpi^{n-1} \\ \dots & \dots & \dots & \dots \\ 1 & \varpi^{n-1} & \dots & \varpi^{(n-1)^2} \end{pmatrix} (\lambda_i')$$

alors $c_i = \frac{1}{n} \sum_{j=0}^{n-1} \lambda_j' \, \varpi^{kj}$; c'est la forme de la transformée de Fourrier Discrete inverse.

2-3 Produit de convolution (discret) :

2-3-1 Definition :

En mathématiques , le produit de convolution de deux vecteurs v et v' se note généralement par "*" et s'écrit : $v * v' = (c_{m)}$

avec $c_m = \sum_{i=0}^{m} a_i b_{m-i}$; avec $v = (a_0, \dots, a_{n-1})$ et $v' = (b_0, \dots, b_{n-1})$.

Exemple :

Soit :

$$v = (a_0, a_1, a_2) \quad ; \quad v' = (b_0, b_1, b_2)$$

alors :

$$v * v' = (a_0, a_1, a_2) * (b_0, b_1, b_2) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + b_0 a_2 + a_1 b_1)$$

2-3-2 Propriétés du produit de convolution :

- Le produit de convolution est commutatif :

$$v * v' = v' * v$$

- Le produit de convolution est distributif par rapport à la somme.

$$u * (v + v') = u * v + u * v'$$

- Le produit de convolution de v et v' correspond à l'image par F^{-1} du produit (discrèt) des transformeés de fourier des vecteurs v et v'

$$v * v' = F^{-1}(F(v).F(v'))$$

où F désigne la transformation de fourier et F^{-1} la transformation de fourier inverse.

- L'intérêt principal de l'utilisation de la transformée de fourier discrète est le gain dans le coût du calcul :

le calcul du produit de convolution (assez couteux) est remplacé par un produit simple (composante par composante).

2-4 Matrices de Toeplitz :

2-4-1 Définition :

En algèbre linéaire une matrice de Toeplitz ou matrice à diagonales constantes est une matrice carrée de type $n \times n$ dont les coefficients $(a_{i;j})$ vérifie l'égalité

$$a_{i;j} = a_{i-1;j-1} \text{ pour tout } 1 \leq i \leq n \text{ et } 1 \leq j \leq n$$

Exemple :

La matrice suivante est une matrice de Toeplitz

$$\begin{pmatrix} a & b & c & d & e \\ f & a & b & c & d \\ g & f & a & b & c \\ h & g & f & a & b \\ j & h & g & f & a \end{pmatrix}$$

•Toute matrice A à m lignes et n colonnes de la forme :

$$A = \begin{pmatrix} a_0 & a_{-1} & a_{-2} & \dots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & \dots & . \\ a_2 & a_1 & a_0 & \dots & a_{-2} \\ . & . & . & . & . \\ . & . & . & . & . \\ a_{m-1} & .... & a_2 & a_1 & a_0 \end{pmatrix}$$

est une matrice de Toeplitz .Si l'élément situé à l'intersection des ligne i et colonne j de A est noté A_{ij} alors on a :

$A_{ij} = a_{i-j}$. Donc toute matrice de Toeplitz est de la forme

$$T = (t_{i-j})_{i,j=0}^{n-1}$$

Remarque :

La notion des matrices de Toeplitz est une généralisation de la notion des matrices circulantes.

Les matrices de Toeplitz sont des matrices dont les entrées sont constante le long de leurs diagonales.

Cette structure est très intéressante en soi pour toutes les propriétés théoriques riches qu'elle entraîne,mais en même temps il est important pour l'impact considerable qu'il a dans les applications.

Les matrices de Toeplitz se posent dans de nombreux domaines théoriques et applicatives différentes, dans la modélisation mathématique de tous les problèmes où une sorte d'invariance de décalage se produit en termes d'espace ou de temps.

Cette invariance de changement se reflète dans la structure de la matrice elle-même où un décalage vers gauche -droite des entrées quitte la matrice inchangé.

La structure Toeplitz peut se produire entrée-sage,pour des problèmes unidimensionnels ou bloc-sages,pour des problèmes bidimensionnels, voire à plusieurs niveaux imbriqués dans les problèmes multidimensionnels.

Problèmes modélisés par des matrices de Toeplitz

Les problèmes typiques modélisés par des matrices de Toeplitz sont les suivants:

La résolution numérique de certaines équations différentielles.

Certaines équations intégrales (régularisation des problèmes inverses);

Analyse de série temporelle.

Traitement du signal et d'image.

Les chaînes de Markov et de la théorie de files d'attente.

Calculs des séries de la puissance et polynômes .

D'autres problèmes concernent les matrices Toeplitz-like ou des matrices ayant une structure de déplacement (Hankel, Bezout, Cauchy, Hilbert, Loewner et matrices de Frobenius).

Il existe une correspondance entre les problèmes impliquant la structure des Toeplitz-like et polynômes (série de puissance) qui permet un passage d'algorithmes de calcul pour Toeplitz-like à des algorithmes de calcul de polynômes et vice-versa (série puissance). De cette façon, Fast Fourier Transform (FFT) devient un outil fondamental pour tous les calculs impliquant des matrices Toeplitz-like.

Exemples :

A. Matrice de Frobenius

Une matrice de Frobenius est une matrice de forme spéciale utilisée dans des applications numériques. Elle possède les propriétes suivantes :

1. Tous les éléments de la diagonale principlale sont des 1.

2. Les éléments d'une colonne au plus sont arbitraires au dessous de la diagonale et les éléments restant sont nuls.

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & b & 0 & 1 \end{pmatrix}$$

est une matrice de Frobenuis d'ordre 4.

On remarque que multiplier à gauche une matrice A par une matrice de Frobenuis revient a utiliser une opération élémentaire de Gauss sur des lignes de A:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & b & 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix} =$$

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31}+aa_{21} & a_{32}+aa_{22} & a_{33}+aa_{23} & a_{34}+aa_{24} \\ a_{41}+ba_{21} & a_{42}+ba_{22} & a_{43}+ba_{23} & a_{44}+ba_{24} \end{pmatrix}$$

B. Matrice de Hankel

Une matrice de Hankel est une matrice H constante sur les diagonales ascendantes et dont les éléments verifient la relation

$$h_{ij} = h_{i-1;\ j+1}$$

Par exemple une matrice de Hankel de taille 4 s'écrit sous la forme

$$\begin{pmatrix} a & b & c & d \\ b & c & d & e \\ c & d & e & f \\ d & e & f & g \end{pmatrix}$$

On remarque qu'une matrice de Hankel carré d'ordre n est une matrice symétrique et que si on multiplie à gauche ou à droite la matrice J_n par une matrice de Hankel on obtient une matrice de Toeplitz :

$$J_n = \begin{pmatrix} 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & \dots & 0 \\ . & . & . & . & . \\ . & . & . & . & . \\ 1 & 0 & 0 & \dots & 0 \end{pmatrix}$$

$$\begin{pmatrix} a & b & c & d \\ b & c & d & e \\ c & d & e & f \\ d & e & f & g \end{pmatrix}\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} d & c & b & a \\ e & d & c & b \\ f & e & d & c \\ g & f & e & d \end{pmatrix} :$$

$$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}\begin{pmatrix} a & b & c & d \\ b & c & d & e \\ c & d & e & f \\ d & e & f & g \end{pmatrix} = \begin{pmatrix} d & e & f & g \\ c & d & e & f \\ b & c & d & e \\ a & b & c & d \end{pmatrix}$$

2-4-2 Propriétés des matrices de Toeplitz : [4],[5]

1- soit $Ax = b \quad (*)$ une équation matricielle.

a/ Dans le cas général :

- Nous savons que $(*)$ correspond à un système de n équations linéaires.
- Il contient n^2 informations .

b/ Cas particulier : A est une matrice de Toeplitz :

- il ne contient que $2n-1$ informations arrangées d'une manière bien particulière .

2- Le produit de deux matrices de Toeplitz n'est pas en générale de Toeplitz .

Exemple :

Soient T_1 et T_2 les matrices d'ordre 3 à coefficients complexes définies par

$$T_1 = \begin{pmatrix} 2 & 1 & -1 \\ 5 & 2 & 1 \\ 0 & 5 & 2 \end{pmatrix} \qquad \text{et} \qquad T_2 = \begin{pmatrix} -1 & 0 & -3 \\ 4 & -1 & 0 \\ 2 & 4 & -1 \end{pmatrix}$$

Alors

$$T_1 T_2 = \begin{pmatrix} 2 & 1 & -1 \\ 5 & 2 & 1 \\ 0 & 5 & 2 \end{pmatrix} \begin{pmatrix} -1 & 0 & -3 \\ 4 & -1 & 0 \\ 2 & 4 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -5 & -5 \\ 5 & 2 & 16 \\ 24 & 3 & -2 \end{pmatrix}$$

3- L'inverse d'une matrice de Toeplitz n'est pas une matrice de Toeplitz sauf pour les matrices triangulaires .[6]

Exemple :

L'inverse de la matrice T_1 donné dans l'exemple précédent est

$$T_1^{-1} = \begin{pmatrix} \frac{1}{37} & \frac{7}{37} & -\frac{3}{37} \\ \frac{10}{37} & -\frac{4}{37} & \frac{7}{37} \\ -\frac{25}{37} & \frac{10}{37} & \frac{1}{37} \end{pmatrix}$$

mais l'inverse de la matrice de Toeplitz triangulaire suivante

$$\begin{pmatrix} -1 & 2 & -3 \\ 0 & -1 & 2 \\ 0 & 0 & -1 \end{pmatrix} \text{ est } \begin{pmatrix} -1 & -2 & -1 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}$$

Chapitre 3 :
Caractères d'un groupe fini

Chapitre 3

3- Caractères d'un groupe fini .

3-1 Définition :

Soit $(G,.)$ un groupe fini .

Définition 1 :

On appelle caractère de G tout homomorphisme χ de $(G,.)$ dans le groupe multiplicatif $\mathbb{C}^*$:

$$\chi : G \rightarrow \mathbb{C}^*$$

comme χ est un homomorphisme alors $\chi(x^m) = (\chi(x))^m$,

$\forall x \in G, \forall n \in \mathbb{N}$,en particulier si $|G| = n$ alors

$\chi(x^n) = \chi(1) = 1 = (\chi(x))^n$ donc $\chi(x) \in u_n$ le groupe des racines n-ième de l'unité.

ceci nous conduit à simplifier la définition 1 comme suit :

Définition 2 :

si G est d'ordre n , χ est un caractère de G si χ est un homomorphisme de G dans u_n .

soit $\hat{G}$ l'ensemble des caractères de G ,on définit le produit dans $\hat{G}$ par $\chi_1 \times \chi_2 : G \rightarrow \mathbb{C}^*$, $\chi_1\chi_2(x) = \chi_1(x)\chi_2(x)$.

alors il est facile à vérifier que $(\hat{G},.)$ est un groupe , il est appelé le dual de G .

3-2 Dual d'un groupe cyclique: $G = \frac{\mathbb{Z}}{n\mathbb{Z}}$

Proposition :

Soit G $=\{1; g_0; g_0^2; \ldots..; g_0^{n-1}\}$ un groupe cyclique de cardinal n et de générateur g_0.

Soit ω une racine primitive n^{ieme} de l'unité, par exemple $\omega = e^{\frac{2i\pi k}{n}}$

Les eléments de $\hat{G}$ sont de la forme, pour $j \in \{0; 1; \ldots; n-1\}$:

$$\chi_j : \begin{cases} G \to \mathbb{C}^* \\ g_0^k \mapsto (\omega^j)^k = e^{\frac{2i\pi jk}{n}} \end{cases}$$

Démonstration :

Pour déterminer un caractère , il nous faut calculer sa valeur sur chacun des eléments de G, c'est- a-dire calculer $\chi(g^k)$ pour $k \in \{0; 1; \ldots; n-1\}$, ce qui donne

$$\chi(g^k) = \chi(g)^k = (\omega^j)^k$$

Dans cette egalité on a noté $\omega^j = \chi(g)$ avec $0 \leq j \leq n-1$ puisque cette quantité est racine n-ième de l'unité. Donc $\chi \in \hat{G}$ est bien un des $\{\chi_0; \ldots; \chi_{n-1}\}$.

Réciproquement, on constate que pour $j \in \{0; \ldots.; n-1\}$ les applications χ_j sont bien des morphismes de G dans $\mathbb{C}^*$, et donc appartiennent bien au dual de G.

Le groupe $\hat{G}$ est cyclique, d'ordre n, engendré par χ_1 (on a $\chi_k = \chi_1^k$).

Proposition :

G et $\hat{G}$ sont isomorphes.

Démonstration :

On identifie les eléments de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ avec leur représentant $j \in \{0; \ldots.; n_1\}$ et on définit l'application suivante :

$$\psi : \begin{cases} \frac{\mathbb{Z}}{n\mathbb{Z}} \to \hat{G} \\ j \mapsto \chi_j \end{cases}$$

Cette application est un morphisme bijectif donc $\hat{G} \simeq \frac{\mathbb{Z}}{n\mathbb{Z}} \simeq G$.
Remarquons toutefois que cet isomorphisme n'est pas canonique, car il dépend de la racine primitive de l'unité ω choisie.

Prenons l'exemple du groupe cyclique $\frac{\mathbb{Z}}{12\mathbb{Z}}$.

On choisit ici comme racine primitive de l'unité $\omega = e^{\frac{2i\pi}{12}}$.

On peut alors définir comme suit les caractères de ce groupe :

$$\chi_0 : (g_0)^k \mapsto 1$$

$$\chi_1 : (g_0)^k \mapsto e^{\frac{ik\pi}{6}}$$

$$\chi_2 : (g_0)^k \mapsto e^{\frac{ik\pi}{3}}$$

$$\chi_3 : (g_0)^k \mapsto e^{\frac{ik\pi}{2}}$$

$$\chi_4 : (g_0)^k \mapsto e^{\frac{2ik\pi}{3}}$$

$$\chi_5 : (g_0)^k \mapsto e^{\frac{5ik\pi}{6}}$$

$$\chi_6 : (g_0)^k \mapsto e^{ik\pi}$$

$$\chi_7 : (g_0)^k \mapsto e^{\frac{7ik\pi}{6}}$$

$$\chi_8 : (g_0)^k \mapsto e^{\frac{4ik\pi}{3}}$$

$$\chi_9 : (g_0)^k \mapsto e^{\frac{3ik\pi}{2}}$$

$$\chi_{10} : (g_0)^k \mapsto e^{\frac{5ik\pi}{3}}$$

$$\chi_{11} : (g_0)^k \mapsto e^{\frac{11ik\pi}{6}}$$

Pour determiner complètement ces caractères, il reste à choisir un genérateur de $\frac{\mathbb{Z}}{12\mathbb{Z}}$.

Les générateurs d'un groupe cyclique additif $\frac{\mathbb{Z}}{n\mathbb{Z}}$ sont les classes d'équivalences des eléments premiers avec n.

Ici on peut donc choisir 1, 5, 7 ou 11 comme générateur, mais nous irons au plus simple en prenant 1.

3-3 Dual d'un groupe abélien fini :

Théorème :[1] , [2]

Soit G_1 et G_2 deux groupes finis.

L'application :

$$f : \hat{G}_1 \times \hat{G}_2 \to G_1 \hat{\times} G_2$$

$$(\chi_1, \chi_2) \to f((\chi_1, \chi_2))$$

où $\chi = f((\chi_1, \chi_2))$ est défini par: $\chi(g_1, g_2) = \chi_1(g)\chi_2(g)$ est un isomorphisme.

Noter que le théorème décrit explicitement les caractères de $G_1 \hat{\times} G_2$ en fonction de ceux de $\hat{G}_1$ et de $\hat{G}_2$.

Corollaire :[1] , [2]

Le dual d'un groupe abélien fini est (non canoniquement) isomorphe à ce groupe; en particulier ils ont même ordre.

Par contre, on a un isomorphisme cette fois canonique entre un groupe G abélien fini et son bidual.

3-4 L'algèbre du groupe $\mathbb{C}[G]$:

On note $\mathbb{C}[G]$ l'ensemble des fonctions $f : G \to \mathbb{C}$, on définit dans cet ensemble deux lois internes :

1) l'addition

$$f + g : (f + g)(x) = f(x) + g(y)$$

2) la multiplication

$$f.g : (fg)(x) = f(x)g(x)$$

3) et une loi externe :

$$\mathbb{C} \times \mathbb{C}[G] \to \mathbb{C}[G]$$

$$(\lambda, f) \to \lambda f$$

Alors il est facile à vérifier que $\mathbb{C}[G]$ est une $\mathbb{C}$ – algèbre , on l'appelle algèbre du groupe .

Soit

$$B = \{\delta_x / x \in G\}$$

Où

$$\delta_x \ : \ G \to \mathbb{C}$$

$$x \to 1$$

$$y \neq x \to \delta_x(y) = 0$$

B est une base nouvelle de $\mathbb{C}[G]$, tout elément $f \in \mathbb{C}[G]$ s'ecrit $\sum_{x\in G} f(x)\delta_x$.

Résultat :

On a :

a) $$dim\ \mathbb{C}[G] = card\ G$$

b) Quand G est commutatif , l'ensemble des caractères de G forme une deuxième base B'de $\mathbb{C}[G]$.

il est possible de munir $\mathbb{C}[G]$ d'un produit hermetien comme suit :

$$\langle f_1, f_2\rangle = \frac{1}{|G|}\sum_{x\in G} f_1(x)\overline{f_2(x)}$$

donc B est une base orthogonale de $\mathbb{C}[G]$,dans ce cas

$$\langle \delta_1, \delta_2\rangle = \frac{1}{|G|} \ \forall x \in G$$

maintenant si on considère la deuxième base B' et on suppose que G est abélien , B'est une base orthonormé pour le produit précédent :

Il faut calculer $< \chi_1, \chi_2 >$ pour deux caractères de G. Remarquons d'abord que $< \chi_1, \chi_2 >=< \chi_1\chi_2^{-1}, 1 >$ En effet .

$$\langle \chi_1, \chi_2\rangle = \frac{1}{|G|}\sum_{x\in G} \chi_1(x)\overline{\chi_2(x)}$$

$$= \frac{1}{|G|}\sum_{x\in G} \chi_1(x)\chi_2^{-1}(x)$$

$$= \frac{1}{|G|}\sum_{x\in G} (\chi_1\chi_2^{-1})(x)$$

$$=< \chi_1\chi_2^{-1}, 1 >$$

En posant $\chi = \chi_1\chi_2^{-1}$, il nous reste à calculer $< \chi, 1 >$. Lorsque $\chi = 1$, on a $\sum_{x\in G} \chi(x) = |G|$ soit$< \chi, 1 >= 1$. Supposons maintenant que $\chi \neq 1$. Il existe donc un élément$b \in G$ tel que $\chi(b) \neq 1$. Comme $hG = G$, on a

$$S = \sum_{x\in G} \chi(x) = \sum_{x\in G} \chi(bx)$$

$$= \sum_{x\in G} \chi(b)\chi(x)$$

$$= \chi(b) \sum_{x\in G} \chi(x) = \chi(b)\ S$$

Soit $S = \chi(b)S$, que l'on peut écrire dans $\mathbb{C}$: $(1 - \chi(b))S = 0$. Comme $\chi\ (b) \neq 1$ on peut en déduire que $S = 0$.

On a donc démontré que les éléments de $\hat{G}$ forment une famille orthonormée.

Comme il y en a exactement $|G|$, ils forment bien une base .

chapitre 4 :

la transformeé de fourier sur un groupe

Chapitre 4

4. La Transformée de Fourier sur un groupe .

On suppose désormais que notre groupe G est abélien fini.

4-1 La transformée de Fourier :

Soit $f \in \mathbb{C}[G]$. On peut décomposer f sur les deux bases orthonormées que l'on connait: $\{\sqrt{|G|}\,\delta_x / x \in G\}$ et $\{x / x \in \hat{G}\}$. Cela donne:

$$f = \sum_{x \in G} f(x)\delta_x = \sum_{x \in \hat{G}} c_f(\chi)\chi$$

où

$$c_f(\chi) = < f, \chi >$$

4-1-1Définition :

On appelle transformée de Fourier de f et on note $\hat{f}$ l'élément de $\mathbb{C}[\hat{G}]$ défini par :

$$\hat{f}(\chi) = |G| c_f(\overline{\chi}) = \sum_{x \in G} f(x)\chi(x)$$

L'application transformée de Fourier, notée F , est:

$$F : \mathbb{C}[G] \to \mathbb{C}[\hat{G}]$$

$$f \quad \to \quad \hat{f}$$

C'est bien sûr un isomorphisme d'éspaces vectoriels.

4-1-2Théorème :[1] , [2]

Soit $f, g \in \mathbb{C}[G]$. On a:

• (**Formule d'inversion**):

$$f = \sum_{x \in \hat{G}} c_f(\chi)\chi = \frac{1}{|G|} \sum_{x \in \hat{G}} \hat{f}(\chi)\chi^{-1}$$

• (**Formule de Plancherel**) :

$$\sum_{x\in G} f(x)\chi(x)\overline{g(x)} = |G|\sum_{x\in \hat{G}} c_f(\chi)\overline{c_g(\chi)} = \frac{1}{|G|}\sum_{x\in \hat{G}} \hat{f}(\chi)\overline{\hat{g}(\chi)}$$

4-2Produit de convolution :

Définition :

Soient f_1 et f_2 deux fonctions définies sur G à valeurs complexes. La convolée de f_1 et de f_2 est la fonction complexe

$f_1 * f_2$ définie sur G par

$$f_1 * f_2(x) = \frac{1}{n}\sum_{y\in G} f_1(x+y)f_2(-y)$$

Il est facile de voir que $f_1 * f_2$ s'écrit aussi :

$$f_1 * f_2(x) = \frac{1}{n}\sum_{y\in G} f_1(y)f_2(x-y)$$

$$f_1 * f_2(x) = \frac{1}{n}\sum_{y\in G} f_1(-y)f_2(x+y)$$

$$f_1 * f_2(x) = \frac{1}{n}\sum_{u+v=x} f_1(u)f_2(v)$$

Théorème :

La transformée de Fourier d'un produit de convolution est le produit (ordinaire) des transformées de Fourier

$$\hat{f_1 * f_2} = \hat{f_1} * \hat{f_2}$$

Preuve

$$\hat{f_1 * f_2} = \frac{1}{n}\sum_{u\in G} f_1 * f_2(x)\overline{\chi(u)}$$

$$\hat{f_1 * f_2} = \frac{1}{n^2}\sum_{u\in G}\Big(\sum_{a+b=u} f_1(a)f_2(b)\Big)\overline{\chi(u)}$$

$$\hat{f_1 * f_2} = \frac{1}{n^2}\sum_{u\in G}\Big(\sum_{a+b=u} f_1(a)\overline{\chi(a)}f_2(b)\Big)\overline{\chi(b)}$$

et la dernière expression correspond bien au produit de b $f_1\hat{}(\chi)$ par b $f_2\hat{}(\chi)$.
Il suffit de revenir à la définition pour voir que

Théorème : [1] , [2]

Le symétrique d'un produit de convolution est le produit de convolution des symétriques

$$f_1\check{} * f_2 = \check{f_1} * \check{f_2}$$

En utilisant les résultats précédents on peut également vérifier que

Théorème : [1] , [2]

La transformée de Fourier d'un produit de fonctions est n fois le produit de convolution des transformées de Fourier

$$f_1\hat{} * f_2 = n\, \hat{f_1} * \hat{f_2}$$

Chapitre 5 :
Variantes de la Transformée de Fourier

Chapitre 5

5.Variantes de la Transformée de Fourier .

5-1 La transformée de Fourier discrète :

La transformée de Fourier discrète (DFT) est extrêmement utile en théorie du signal. C'est en fait une transformée de Fourier sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

et on peut en calculer les valeurs par un algorithme rapide (FFT)analogue .

Définition :

Soit :

$$w_N = e^{\frac{2\pi i}{N}}$$

L'application DFT_N est définie par:

$$DFT_N \ : \ \mathbb{C}^N \to \mathbb{C}^N$$

$$f \ \mapsto \hat{f}$$

où :

$$\hat{f}\ [k] = \sum_{n=0}^{N-1} f[n] w_N^{-nk}$$

Faisons le lien avec la transformée de Fourier définie au Chapitre 4.

Le groupe $G = \frac{\mathbb{Z}}{n\mathbb{Z}}$ a pour caractères les applications: χ_k définies par:

$$\chi_k(n \ mod \ N) = w_N^{-nk}$$

Notons encore f l'application de $\frac{\mathbb{Z}}{n\mathbb{Z}}$ dans $\mathbb{C}$ associée à $f = (f[0],\ldots,f[N-1])$, c'est-à-dire $f(k \ mod \ N) = f[k]$. Alors il est clair que:

$$(DFT_N f)[k] = (Ff)(\chi_f)$$

Pour cette raison, on note de la même façon:

$$\hat{f} \ = DFT_N f = Ff$$

Les résultats du Chapitre 4 s'applique en particulier à la transformée de Fourier discrète; ainsi, la fornmule d'inversion (Thèorème *) montre que DFT est inversible et que DFT^{-1} est encore une DFT, où on a remplacé w_N par w_N^{-1}.

En termes matriciels, notons V_{w_N} la matrice de taille $N \times N$ définie par : $V_{w_N}[i,j] := w_N^{(i-1)(j-1)}$ pour tout $1 \leq i, j \leq N$.

La matrice de DFT_N dans la base canonique de $\mathbb{C}^N$ est V_{w_N} et celle de DFT_N^{-1} est $\frac{1}{N} V_{w_N^{-1}}$ On a bien sûr :

$$V_{w_N} V_{w_N^{-1}} = N\, Id_N$$

La formule de Plancherel (Thèorème *) devient:

$$\sum_{k=0}^{N-1} f[n]\overline{g[k]} = \frac{1}{N} \sum_{k=0}^{N-1} \hat{f}\,[n]\overline{\hat{g}\,[k]}$$

En termes matriciels, la matrice : $\frac{1}{\sqrt{N}} V_{w_N}$ est unitaire .

5-1-1 Représentation matricielle :

Soient $X_0, \ldots, X_{n-1}$ des nombres complexes.

La transformée de Fourier discrète est définie par la formule suivante :

ou en notation matricielle :

$$\begin{pmatrix} f_0 \\ f_1 \\ f_2 \\ \vdots \\ f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{n-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{n-1} & \omega^{2(n-1)} & \cdots & \omega^{(n-1)^2} \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ \vdots \\ x_{n-1} \end{pmatrix}, \omega = e^{\frac{-2i\pi}{n}}$$

5-1-2 Discrétisation et quantification du signal :

A. Discrétisation

Soit $f(t)$ un signal analogique .

La discrétisation de ce signal revient à n'en garder qu'un certain nombre de valeurs $(\ldots, f_{-1}, f_0, f_1, \ldots)$ correspondant aux valeurs $(\ldots, t_{-1}, t_0, t_1, \ldots)$ de la variable t:

On ne dispose donc plus, après discrétisation, que d'une suite $(fn)_Z$, où Z désigne l'ensemble des entiers relatifs. On appelle cette suite un signal discret associé au signal analogique $f(t)$.

Dans la quasi-totalité des cas, l'échantillonnage est périodique, c'est-à-dire que ...$= t_0 - t_{-1} = t_1 - t_0 = \ldots = T_e$, valeur qu'on appelle la période d'échantillonnage. On définit aussi la pulsation d'échantillonnage par :

$$w_e = \frac{2\pi}{T_e}$$

Un problème majeur en traitement du signal est le choix de cette pulsation d'échantillonnage w_e :

Si w_e est trop grand, on aura trop de données à traiter et à stocker.

Si w_e est trop petit, la suite $(fn)_Z$ ne sera pas fidèle au signal initial $f(t)$.

Nous verrons un peu plus loin qu'il existe un critère optimal pour choisir cette pulsation, qui s'appelle le "critère de Shannon".

B. Quantification

La quantification est une opération qui modifie légèrement les valeurs du signal discret précédent.

Ceci vient du fait qu'en informatique, les supports d'information ne sont pas analogiques mais binaires, et que donc toute valeur réelle ne peut pas être mémorisée.

On obtient donc, après quantification, une suite $(fn)_Z$ telle que, pour tout entier n. $f'_n \approx f_n$

Remarques :

On dit parfois que la discrétisation est une "discrétisation en abscisse", alors que la quantification est une "discrétisation en ordonnée".

La quantification introduit une erreur dans les valeurs du signal, ce que ne fait pas la discrétisation.

La discrétisation fait-elle perdre de l'information ?

On a vu qu'il était très simple de passer d'un signal analogique f(t) au signal discret correspondant $(fn)_Z$, pourvu qu'une pulsation d'échantillonnage w_e ait été choisie.

Notions :

Modélisation de l'échantillonnage

L'opération mathématique associée à cette discrétisation revient à multiplier le signal $f(t)$ par un peigne de Dirac $\delta_{T_e}(t)$:

$$f^*(t) = f(t)\delta_{Te}(t) = f(t)\sum \delta(t - nT_e)$$

On peut ainsi calculer la transformée de Fourier du signal échantillonné en utilisant les propriétés liant une multiplication temporelle qui dans l'espace fréquentiel devient un produit de convolution :

$$TF(f(t).P_{Te}(t) \rightarrow F^*(f) = \frac{1}{T_e}F(f) * \delta_{fe=\frac{1}{T_e}}(f)$$

soit :

$$F^*(f) = \frac{1}{T_e}\sum_{k=-\infty}^{+\infty} F(f - kfe)$$

Echantillonner le signal $f(t)$ dans le domaine temporel, revient donc à recopier dans le domaine fréquentiel son spectre $F(f)$ tous les w_e

Notion de repliement de spectre

On remarquera que si le spectre du signal d'origine à une largeur supérieur à $2w_e$ on a ce qu'on appelle un repliement de spectre ce qu'on appelle un repliement de spectre.

S'il y a repliement de spectre, il n'est plus possible de retrouver le spectre du signal d'origine.

Dans ce cas, l'opération d'échantillonnage modifie les caractéristiques du signal d'entrée.

Ainsi, si l'on ne veut pas perdre d'informations par rapport au signal que l'on échantillonne, on devra toujours respecter la condition : ($w_e \geq 2w\ max$).

Condition plus connue par le théorème de Shannon.

Théorème de Shannon :[14] ; [15]

On ne peut échantillonner un signal sans pertes d'informations que si :

$$w_e \succ 2w_{max}$$

5-2 Transformée de Fourier rapide :

Il existe divers façons proches les une des autres de calculer une transformée de Fourier discrète.

Toutes ces variantes sont des algorithmes de transformée de Fourier rapides (FFT).

Nous nous placerons ici dans le cas où le nombre d'éléments du groupe est $n = 2^m$ et où le groupe G est $\frac{Z}{n\mathbb{Z}}$.

Pour tout $r > 0$ et tout $0 \leq k \leq 2^r - 1$ posons

$$W_{2^r}^k = e^{\frac{-2ik\pi}{2^r}}$$

Remarquons que

$$W_{2^r}^k = (W_{2^{r+1}}^k)^2 = (W_{2^{r+1}}^{k+2^r})^2$$

$$W_{2^{r+1}}^k = -W_{2^{r+1}}^{k+2^r}$$

par exemple

$$W_8^1 = (W_{16}^1)^2 = (W_{16}^9)^2$$

$$W_{16}^1 = -W_{16}^9$$

On rappelle que si

$$f = (a_{0,}a_1,\ldots,a_{2^m-1}), \text{ et si } \; p_f(X) = \frac{1}{2^m}(a_0 + a_1X,\ldots,a_{2^m-1}X^{2^m-1})$$

alors

$$\widehat{f(u)} = \widehat{a_u} = p_f(\quad W_{2^m}^u)$$

Pour tout polynôme

$$P(X) = p_0 + p_1X + \ldots + p_{2^r-1}X^{2^r-1}$$

notons

$$P_0(X) = p_0 + p_2X + \ldots + p_{2^r-2}X^{2^{r-1}-1}$$

et

$$P_1(X) = p_1 + p_3X + \ldots + p_{2^r-1}X^{2^{r-1}-1}$$

alors

$$P(X) = P_0(X^2) + XP_1(X^2)$$

ce qui donne si

$$0 \leq k \leq 2^{r-1} - 1$$

$$\mathbb{P}(\mathbb{W}_{2^r}^k) = \mathbb{P}_0(\mathbb{W}_{2^{r-1}}^k) + \mathbb{W}_{2^r}^k\mathbb{P}_1(\mathbb{W}_{2^{r-1}}^k)$$

et

$$P(W_{2^r}^{k+2^{r-1}}) = P_0(W_{2^{r-1}}^k) - W_{2^r}^kP_1(W_{2^{r-1}}^k)$$

Ces dernières formules vont nous donner un algorithme pour calculer les valeurs de la transformée de Fourier.

5-3 Transformation de Fourier sur $\frac{\mathbb{Z}}{n\mathbb{Z}}$: [16]

On se place donc dans le cas où $G = \frac{\mathbb{Z}}{n\mathbb{Z}}$. Dans ce cas les caractères de G sont les fonctions

$$\chi_u(v) = e^{\frac{-2i\pi uv}{n}}$$

Ces fonctions sont indexées par les entiers$u$ compris entre0 et $n-1$ si bien qu'une transformée de Fourier apparaît ici comme fonction d'un tel entier.

Plus précisément si $f \in F(G)$, notons

$$a_u = f(u) \text{ où } u = 0, 1, \ldots, n-1$$

Dans ces conditions

$$\hat{f}(v) = \langle f, \chi_v \rangle = \frac{1}{n} \sum_{u=0}^{n-1} a_u e^{\frac{-2i\pi uv}{n}}$$

$$f(u) = \sum_{v=0}^{n-1} \hat{f}(v) e^{\frac{2i\pi uv}{n}}$$

En ce qui concerne la convolution, il est intéressant de noter qu'elle s'interprète à l'aide du produit de polynômes.

Pour cela si f est la fonction dont les images sont $a_0, a_1, \ldots, a_{n-1}$, et h celle dont les images sont $b_0, b_1, \ldots, b_{n-1}$, notons

$$P_f(X) = \frac{1}{n}(a_0 + a_1 X, \ldots, a_{n-1} X^{n-1})$$

$$P_h(X) = \frac{1}{n}(b_0 + b_1 X, \ldots, b_{n-1} X^{n-1})$$

On sait que

$$f * h(u) = \frac{1}{n} \sum_{\substack{i+j=u(n) \\ 0 \le i \le n-1 \\ 0 \le j \le n-1}} a_i b_j$$

donc

$$P_{f*h} = p_f p_h mod(x_n - 1)$$

Remarquons en outre que

$$\hat{f}(u) = P_f(e^{\frac{-2i\pi u}{n}})$$

Cette dernière remarque met en évidence un aspect très important de la transformée de Fourier discrète : l'aspect interpolation. En effet il est facile de trouver grâce à ce que nous avons vu un polynôme trigonométrique

$$P(x) = \sum_{u=0}^{n-1} \beta_u e^{iux}$$

qui interpole une fonction donnée aux points $x_V = \frac{2v\pi}{n}$

Nous verrons par la suite le lien qui existe entre ce polynôme trigonométrique et les sommes partielles de la série de Fourier de la fonction.

5-4 Transformation d'Hadamard : [16]

La transformation d'Hadamard relève du cas particulier où $G = \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^m$ Dans ce cas là a les caractères de G sont les fonctions définies par :

$$W_x(y) = (-1)^{<x,y>}$$

(ces fonctions sont les fonctions de Walsh). Nous pouvons indexer les caractères en utilisant la décomposition binaire des nombres.

Ainsi on peut supposer que l'élément $x = (x_1, x_2, \ldots, x_m) \in G$ représente le nombre entier compris entre 0 et $2^m - 1$

$$x_1 + 2x_2 + \ldots + (2^m - 1)x_m$$

Comme cas particulier soit $x = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$où $x_j = 1$ et $x_i = 0$ si $i \neq j$. On obtient alors la fonction de Rademacher d'ordre j(où $1 \leq j \leq n$)

$$r_j(y) = W_{2^{j-1}}(y) = \begin{cases} 1 \text{ si } y_j = 0 \\ -1 \text{ si } y_j = 1 \end{cases}$$

Si besoin est on posera $r_0 = 1$. Les fonctions de Walsh sont des produits de fonctions de Rademacher. Plus précisément

$$W_\lambda = \prod_{j=1}^{n} r_j', \mathrm{r}_j' = \begin{cases} r_j \text{ si } \lambda_j = 1 \\ 1 \text{ si } \lambda_j = 0 \end{cases}$$

En reprenant la définition générale de la transformation de Fourier nous voyons que la transformation d'Hadamard s'écrit (très simplement) sous la forme

$$\hat{f}(x) = \frac{1}{2^m} \sum_{y=0}^{2^m-1} f(y)(-1)^{<x,y>}$$

et

$$f(y) = \sum_{x=0}^{2^m-1} \hat{f}(x)(-1)^{<x,y>}$$

A partir des fonctions de Rademacher on peut définir une autre base orthonormée intéressante : les fonctions de Haar.

5-5 Transformation de Fourier sur $(\frac{Z}{nZ})^m$: [16]

Dans ce cas G est le groupe produit $(\frac{Z}{nZ})^m$.

Soit f une fonction complexe définie sur G, notons pour tout élément $u = (u_1, u_2, \ldots, u_m)$ de G

$$a_{u_1,u_2,\ldots,u_m} = f(u)$$

et

$$P_f(X_1, X_2, \ldots, X_m) = \frac{1}{n} \sum_{u \in G} a u_1, u_2, \ldots, u_m X_1^{u1}, X_2^{u_2}, \ldots, X_m^{u_m}$$

On sait que les caract'eres de G sont indexés par les éléments de G et on peut écrire

$$\hat{f}(u) = \frac{1}{n} \sum_{v \in G} a_v e^{\frac{-2i\pi <u,v>}{n}}$$

c'est-à-dire encore

$$\hat{f}(u) = P_f(e^{\frac{-2i\pi u_1}{n}}, e^{\frac{-2i\pi u_2}{n}}, \ldots, e^{\frac{-2i\pi u_m}{n}})$$

Il est aussi facile de constater que si ζ est l'idéal engendré par les polynômes $X_s^n - 1$ (où $s = 1, \ldots, m$) alors

$$P_{f*h}(X_1, X_2, \ldots, X_m) = P_f(X_1, X_2, \ldots, X_m) P_h(X_1, X_2, \ldots, X_m) \text{mod}(\zeta)$$

5-6 Transformée de fourier sur les corps finis :

5-6-1 Rappel sur les corps finis :

soit F un ensemble non vide et fini muni de deux lois internes :

- $F(+)$ est un groupe abélien .
- $F(+;\times)$ est un anneau où tout élément sauf 0 par $\times$ admet un inverse .

Exemple :

$\frac{\mathbb{Z}}{p\mathbb{Z}} = \{0, 1, \ldots., p-1\}$ avec p premier sont des corps fini de cardinal p .

Proposition :[13]

soit K un corps fini à p élément alors

$$\forall x \in K : x^p = x$$

Théorème :[13]

$\mathbb{F}_{p^n}$ est le corps de rupture de tout polynôme irréductible de degré n sur $\frac{\mathbb{Z}}{p\mathbb{Z}}$.

5-6-2 Exemple de construction d'un corps fini :

a/ Représentation primitive

Soit $\mathbb{F}_8$ un corps fini , on a $\mathbb{F}_8 = \mathbb{F}_{2^3}$, $\mathbb{F}_2 = \{0,1\}$ prenons le polynome primitif $f(x) = 1 + x + x^3$

Le corps admet huit éléments donc il contient un élément β d'ordre 7 qui est une racine primitive de l'unité.

$\mathbb{F}_8 = \{0,,\beta,\beta^2,\beta^3,\beta^4,\beta^5,\beta^6,\beta^7 = 1\}$ et β est racine du polynôme $(x^7 - 1)$ mod 2

On à :

$$1 + x + x^3 = 0$$

$$x^3 = 1 + x$$

$$x^4 = x + x^2$$

$$x^5 = x^2 + x^3 = x^2 + x + 1$$

$$x^6 = x^3 + x^2 + x = 1 + x + x^2 + x = 1 + x^2$$

$$x^7 = x^3 + x = 1 + x + x = 1$$

Donc

$$\mathbb{F}_8 \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}[x] \,/\, (1 + x + x^3)$$

et de même on construit les corps suivants

$$\mathbb{F}_9 \simeq \frac{\mathbb{Z}}{3\mathbb{Z}}[x] \,/\, (1 + x^2)$$

$$\mathbb{F}_{16} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}[x] \,/\, (1 + x + x^4)$$

b/ Représentation vectoriale (polynomiale) :

$$\mathbb{F}_8 = \{a + bx + cx^2 / a,b,c \in \mathbb{F}_2\}$$

$$= \begin{cases} 0,1,x,1+x,1+x^2,1+x+x^2,x+x^2,x^2, \\ \text{où x est une racine primitive } 7 = \text{ ime de l'unite} \end{cases}$$

Remarque :

Pour le calcul de l'addition on préfere utiliser la représentation vectoriale, pour le produit on utilise la représentation primitive .

Définition :

Soit $\mathbb{F}_q$ un corps fini tell que $q = p^m$; alors

$$TFD \text{ de long } n \iff n \; div \; q-1 \iff n \; div \; p^m - 1 \; (p^m \equiv 1[n])$$

On cherche le plus petite valeur de m tel que $(*)$ est vérifié.

Exemple :

Soient $\mathbb{F}_q$ un corps fini de cardinal $n = 27$ alors :

$$TFD \text{ de long } n \implies n \text{ divise } q-1$$

on à :

$$27 \text{ div } p^m - 1 \; / \; q = p^m \text{ donc } \exists m ? : 2^m \equiv 1[27]$$

on à :

$$2 \equiv 2[27]$$

$$2^2 \equiv 4[27] \qquad 2^3 \equiv 8[27]$$

$$2^4 \equiv 16[27] \qquad 2^5 \equiv 5[27]$$

$$2^6 \equiv 10[27] \qquad 2^{17} \equiv 14[27]$$

$$2^8 \equiv 13[27] \qquad 2^9 \equiv 26[27]$$

$$2^{10} \equiv 25[27] \qquad 2^{11} \equiv 23[27]$$

$$2^{12} \equiv 19[27] \qquad 2^{13} \equiv 11[27]$$

$$2^{14} \equiv 22[27] \qquad 2^{15} \equiv 17[27]$$

$$2^{16} \equiv 7[27] \qquad 2^{17} \equiv 14[27] \qquad 2^{18} \equiv 1[27]$$

Le plus petit corps fini dans lesquel on peut définir un TFD de longeur 27 est 2^{18} , $\mathbb{F}_{2^{18}}, \omega^{2^{18}-1} = 1$

$$\omega \in \mathbb{F}_q = \mathbb{F}_{2^{18}} \ , \ \omega^{27} = 1 \Rightarrow \circlearrowleft(\omega) = 27$$

$$u = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \omega & \dots & \omega^{26} \\ \dots & \dots & \dots & \dots \\ 1 & \omega^{26} & \dots & \omega^{26^2} \end{pmatrix}$$

5-7 les applications de la transformée de Fourier discrète :

5-7-1 Produits de deux entiers :

Soit A et B deux polynômes de degré $n < \frac{N}{2}$
En $O(logn)$ opération tel que

$$A = \sum_{i=0}^{n-1} a_i x^i$$

$$B = \sum_{i=0}^{n-1} b_i x^i$$

et

$$R = A \cdot B = \sum_{i=0}^{2n} r_i X^i$$

On utilise une transformée de Fourier de taille $N = 2n$ avec les vecteurs :

$$a = (a_0, a_1, \dots, a_{n-1}, 0, 0, \dots, 0_n termes).$$

$$b = (b_0, b_1, \dots, b_{n-1}, 0, 0, \dots, 0_n termes).$$

Soit ω une racine primitive $2n - ieme$ de l'unité la transformée de a

$$F_\omega(a) = (à_0, à_1 ; \dots à_{2n-1})$$

N'est autre que :

$$(a(\omega^0), a(\omega^1), \dots a(\omega^{2n-1}))$$

De même pour b, de sorte que le produit terme à terme des deux vecteurs :

$$F\omega(a) * F_\omega(b) = (à_0 b'_0, à_1 b'_1, \dots à_{2n-1} b'_{2n-1}).$$

Donne en fait les valeurs de

$$R(x) = A(x)B(x) = T^{-1}(à_0 b\prime_0, à_1 b\prime_1, \ldots à_{2n-1} b\prime_{2n-1}).$$

en les racine de l'unité c.à.d.

$$F_\omega(R), \omega = e^{\frac{2i\pi}{N}}$$

5-7-2 Compression d'images : [17]

Définition de la CDT

Soit :

$$f_0 : \{0, \ldots, N-1\} \rightarrow \mathbb{R}$$

$$f(n) = f_0 \text{ (reste de la division de n par N)}$$

alors pour tout v, n tels que . $0 \leq v, n < N$.

$$DCT(f)(V) = \left(\frac{C(v)}{\sqrt{N}}\right) \sum_{0 \leq n < N} f(n) \cos\left(\frac{\pi v(2n+1)}{2N}\right)$$

$$C(v) = \begin{cases} 1 \text{ si } v = 0 \\ \sqrt{2} \quad sinon \end{cases}$$

le principe :

On choisit un paramètre $q \in [1, +\infty[$ dit de (quantification) on divise les valeurs de $DCT(f)$ par q et on arrondit à l'entier le plus proche . Ces nouvelles valeurs sont appelées «valeurs quantifiées» Cela a pour effet d'annuler les valeurs $< \frac{q}{2}$, ce qui sera le cas pour le grandes de V. Pour une image, cela permet d'identifier les zones contigües de couleurs voisines (mise en évidence de corrélations entre les pixels). Cela a aussi pour effet d'introduire un certain nombre de zéros dans la représentation des données que l'on peut de nouveau compresser. (sans perte) via une méthode d'agrégation de zéros le principe en est le suivant :

Supposons que l'on ait une suite consécutive de m zéros $\underbrace{(0, 0, \ldots, 0)}_{m \text{ zéros}}$

Alors on l'encode sous la forme $m \times 0$

Ainsi, si l'on a juste un zéro, on ajoute une donnée supplémentaire, mais génériquement on réduira la taille.

En complément, on appliquera aussi un codage de Hoffman qui permet de nouveau de faire une compression sons perte les formats MP3. Ogg. vorbis, speese (format audio utilisé eu téléphonie).

JPEG, MPEG − 1, MPEG − 2Divx utilisent les procédés d'écrits ci-dessus le format JPE. G2000 utilise des transformations par ondelettes au lieu de la DCT .

Remarque :

DCT est la partie réel de *TFD* tel que *TFD* est notée :

$$X_k = \sum_{n=0}^{N-1} f_n e^{\frac{-2i\pi kn}{N}}$$

Le calcul de la *DCT* se déduit de celui de la *TFD*

DCT est plus précis que TFD.

Formule pour calculer la DCT sur une matrice NxN : [16]

$$DCT(i,j) = \frac{1}{\sqrt{2}} c(i)c(j) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} pixel(x,y) \cos\left(\frac{\pi i(2x+1))}{2N}\right) \cos\left(\frac{\pi j(2y+1)}{2N}\right)$$

5-7-3 Tatouage d'images :

On a le plan suivant :

Image originale I (hôte) $\overset{TFD}{\Rightarrow} I'$, on ajoute $\alpha\omega_i$ a' des valeurs particulières de $I' \Rightarrow I_1$ image tatouée (elle contient le water mark "la marque" $W(w_1, \cdots, w_{n-1})$)

En pratique (W contient des informations sur le propriétaire), donc le tatouage est utilisé pour la protection des droits d'auteurs .

Résumé

Résumé :

Dans ce travail, on s'est intéressé à l'étude de la transformée de Fourier discrète, notion utile en théorie et en application.

A travers ce thème, on a rappelé les outils mathématiques indispensables pour ce genre d'étude.

Ensuite on a utilisé la notion de caractères pour généraliser la transformée de Fourier à un groupe quelconque, les différentes variantes de la transformée de Fourier son obtenues suivant le groupe de base, des exemples d'application sont donnés.

Abstract :

In this work, we are interested in the study of the discrete Fourier transform, this concept is useful in theory and applications.

Through this theme, we recalled the necessary mathematical tools for this kind of study.

Then we used the notion of characters to generalize the Fourier transform to any group, variants of Fourier transform are obtained according to appropriate group, and examples of applications are given .

الملخص :

في هذه المذكرة نهتم بدراسة " تحويل فوريي المتقطع " ,إن هذا المفهوم مهم من الناحية النظرية و التطبيقية معا .

خلال هذا الموضوع ، عرضنا الأدوات الرياضية الضرورية لهذا النوع من البحث ، بعدئذ استخدمنا مفهوم " التوسيمات " لتعميم تحويل فوريي إلى زمرة كيفية ، وهكذا فإن أنواع تحويلات فورييه المعروفة تظهر كحالة خاصة حسب اختيار الزمرة الأساسية ، وفي الأخير أعطينا أمثلة تطبيقية .

Bibliographie

Bibliographie

[1] Gabriel Peyré, L'algèbre discrète de la transformée de Fourier (ellipses 2004) .

[2] Joachim von zur Gathen, Jürgen Gerhard, Modern computer algebra (second 2004) .

[3] R. M. Gray, "On the asymptotic eigenvalue distribution of Toeplitz matrices,"IEEE Transactions on Information Theory,Vol.18,November 1972, pp.725–730.

[4] R.M. Gray, "On Unbounded Toeplitz Matrices and Nonstationary Time Series with an Application to Information Theory," Information and Control, 24, pp.181–196, 1974.

[5] U. Grenander and G. Szeg¨o, Toeplitz Forms and Their Applications, University of Calif. Press, Berkeley and Los Angeles, 1958.

[6] V. Y. Pan, Z. Q. Chen, Approximate real polynomial division via approximate inversion of real triangular Toeplitz matrices, Applied Mathematics Letters 12 (1999) 1-2.

[7] Bracewell, Ronald N. Convolution Theorem. The Fourier Transform and Its Applications, 3^{e} édition New York : McGraw-Hill, 1999.

[8] Piskounov N. Calcul Différentiel et Intégral, 12e édition Ellipses : éditions Mir Moscou, 1993.

[9] Bellman, R. Introduction to Matrix Analysis, 2nd ed., McGraw-Hill, New York,1970.

[10] Davis, P. J. Circulant Matrices, John Wiley & sons, New York, 1979.

[11] Gilmore, R. Lie Groups, Lie Algebras, and some of their Applications, Wiley, New York, 1974.

[12] Lancaster, P., Tismenetsky, M. The Theory of Matrices 2nd ed,, Academic Press, San Diego, 1985.

[13] Robert Mc Eliece, Finite fields for computer scientists and engineers, Kluwer Academic, 1987. Livre admirable, pour une introduction aux corps finis.

[14] Rudolf Lidl andHarald Niederreiter, Finite fields, Encyclopedia ofMathematics and its Applications, Cambridge University Press, 1997. Extrêmement complet !

[15] A. J. Jerri, "The Shannon sampling theorem - its various extensions and applications : a tutorial review", Proceedings IEEE, Vol. 65, No. 11, November 1977, pp. 1565-1596.

[16] R. Rolland, Association ACrypTA, 50 Rue Edmond Rostand 13006 Marseille, 2006 .

[17] Transformée de Fourier discrète et Applications à la Compression Audio/Vidéo ,Philippe Elbaz-Vincent .