Robert Rolland

GROUPES FINIS COMMUTATIFS ET TRANSFORMATION DE FOURIER DISCRÈTE

Robert Rolland
E-mail : rolland@iml.univ-mrs.fr
Url : http://iml.univ-mrs.fr/~rolland
C.N.R.S. Institut de Mathématiques de Luminy, case 930, F13288 Marseille cedex 9, France..

31 mars 2006

GROUPES FINIS COMMUTATIFS ET TRANSFORMATION DE FOURIER DISCRÈTE

Robert Rolland

CHAPITRE 1

INTRODUCTION

L'étude que nous proposons ici concerne la transformée de Fourier discrète et les notions qui en sont proches. Ces notions sont utiles dans divers domaines des mathématiques théoriques ou appliquées et notamment dans l'étude des signaux (de leur analyse et de leur synthèse), du filtrage, du codage de l'information, domaines que nous aurons plus particulièrement en vue.

Bien que l'étude porte ici sur des signaux discrets (c'est-à- dire connus par un nombre fini de valeurs) il convient d'avoir en perspective l'aspect continu de la question, un signal discret étant en fait souvent une approximation d'un signal continu. Les relations entre l'aspect discret et l'aspect continu ne sont pas toujours très simples à exprimer (et sont souvent très peu développées dans les livres de référence). Par exemple quels sont les liens entre la transformée de Fourier d'une fonction réelle et la transformée de Fourier discrète d'une approximation en un certain nombre de points de cette fonction ?

La transformation de Fourier est une question tellement centrale en mathématiques qu'elle a donné lieu à de nombreuses généralisations et qu'elle touche sous divers aspects de nombreux domaines. Ainsi elle peut être abordée de plusieurs façons et à plusieurs niveaux (transformation de Fourier classique sur $\mathbf{R}^n$, transformation de Laplace bilatère, transformation de Fourier des distributions, transformation de Fourier sur les groupes, algèbres de Banach et transformation de Gelfand). Bien entendu les niveaux d'abstaction des diverses généralisations et les objets

mathématiques mis en œuvre sont aussi très différents. L'exposé que nous avons choisi ici, adapté au cas des fonctions discrètes, met en avant la notion de caractère d'un groupe commutatif et la décomposition d'une fonction sur la base des caractères et plus généralement la décomposition d'une fonction sur des bases bien choisies. Ces notions apparaissent naturellement lorsqu'on s'intéresse par exemple aux filtres linéaires stationnaires.

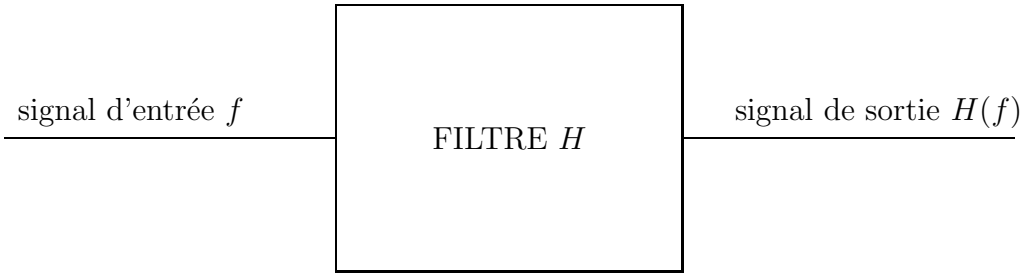

FIGURE 1. Filtre

Soit f une fonction (signal d'entrée) définie sur un groupe fini commutatif G à valeurs complexes et H un filtre linéaire, c'est-à-dire une application linéaire qui à f fait correspondre la fonction $H(f)$ (signal de sortie) elle aussi définie sur G à valeurs complexes. On suppose en outre que ce filtre est stationnaire c'est-à-dire que si on note T_t l'opérateur de translation qui à la fonction f associe la fonction $T_t(f)$ définie par

$T_t(f)(x) = f(x+t)$ alors

$$H(T_t(f)) = T_t(H(f))$$

c'est-à-dire que T_t commute avec H

$$H \circ T_t = T_t \circ H.$$

Il est intéressant de trouver si possible une base de vecteurs propres de H et de décomposer f sur cette base.

Les fonctions χ non nulles qui vérifient

$$\chi(x+y) = \chi(x)\chi(y)$$

sont des vecteurs propres de H. En effet la stationnarité de H implique

$$H(\chi)(x+y) = H(T_x(\chi))(y)$$

mais

$$T_x(\chi)(u) = \chi(x+u) = \chi(x)\chi(u)$$

c'est-à-dire

$$T_x(\chi) = \chi(x)\chi$$

donc en utilisant la linéarité de H

$$H(\chi)(x+y) = \chi(x)(H(\chi)(y))$$

ou encore en prenant $y = 0$

$$H(\chi)(x) = H(\chi)(0)\chi(x)$$

et en posant $\lambda = H(\chi)(0)$ on obtient le résultat

$$H(\chi) = \lambda\chi.$$

Ces considérations expliquent a priori l'importance de l'introduction des caractères du groupe G.

On remarquera aussi que lorsqu'on travaille sur un ensemble fini, si on veut pouvoir calculer et introduire des outils sur cet ensemble il convient de lui donner un minimum de structure, c'est ce que nous faisons en supposant que G est un groupe.

CHAPITRE 2

LES GROUPES FINIS COMMUTATIFS

2.1. Exemples

2.1.1. Le groupe $\mathbf{Z}/n\mathbf{Z}$. — C'est le groupe à n éléments des entiers modulo n (seule l'addition nous intéresse pour le moment, ce qui explique que nous ne parlions que de la structure de groupe).

2.1.2. Le groupe $\{0,1\}^m$. — C'est le produit de m groupes à 2 éléments.

2.2. Les groupes finis commutatifs

En fait, le cas général s'appuie sur les exemples précédents dans la mesure où nous disposons du résultat

Théorème 2.2.1. — *Tout groupe abélien fini G est isomorphe à un produit de groupes $\mathbf{Z}/n_i\mathbf{Z}$. En outre les n_i peuvent être pris comme des puissances de nombres premiers.*

Ainsi

$$G = \prod_{i=1}^{m} \mathbf{Z}/n_i\mathbf{Z}$$

Remarques.
– Attention le groupe $\mathbf{Z}/4\mathbf{Z}$ n'est pas isomorphe au groupe $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$;
– $\mathbf{Z}/6\mathbf{Z}$ est isomorphe à $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$;
On rappelle à ce propos le théorème chinois

***Théorème 2.2.2* (chinois).** — *Soient m et n deux nombres premiers entre eux. Le groupe $\mathbf{Z}/mn\mathbf{Z}$ est isomorphe au produit de groupes $\mathbf{Z}/m\mathbf{Z}\times \mathbf{Z}/n\mathbf{Z}$.*

Le théorème chinois s'exprime aussi de la façon suivante

autre énoncé. Soient m et n deux entiers premiers entre eux, alors pour tout couple (a, b) d'entiers, le système

$$\begin{cases} x & = & a & (m) \\ x & = & b & (n) \end{cases}$$

admet des solutions entières. Deux quelconques de ces solutions diffèrent d'un multiple de mn.

La réalisation d'un tel isomorphisme ϕ peut se faire de la manière suivante :

$$\phi(x) = (x \mod m, x \mod n).$$

Le calcul de ϕ^{-1} utilise le théorème de Bézout et l'algorithme d'Euclide étendu : on commence par calculer u et v tels que $um + vn = 1$. Alors le système précédent admet une solution

$$x = bum + avn.$$

(La vérification est immédiate.)

2.3. Indexation des éléments d'un groupe abélien fini

Comme nous allons le voir dans la suite il est très souvent commode d'avoir une bonne numérotation des éléments d'un groupe fini.

2.3.1. Cas du groupe $\mathbf{Z}/n\mathbf{Z}$. — Dans ce cas là il est très facile de numéroter les éléments car ceux ci peuvent être considérés comme étant les nombres entiers $0, 1, ..., n-1$.

2.3.2. Cas du groupe $\{0,1\}^m$. — Ici, il suffit d'utiliser la décomposition binaire des nombres. Ainsi l'élément $(u_1, u_2, ..., u_m)$ du groupe $\{0,1\}^m$ peut être indexé par le nombre entier $u = \sum_{i=1}^{m} u_i 2^{i-1}$.

2.3.3. Le cas général. — Le principe est le même que précédemment en tenant compte du fait que le groupe G s'écrit sous la forme

$$G = \prod_{i=1}^{m} \mathbf{Z}/n_i\mathbf{Z}.$$

Posons alors $e_1 = 1$ et pour $i > 1$ posons $e_i = \prod_{1 \leq j < i} n_i$.

Dans ces conditions l'élément $(u_1, u_2, ..., u_m)$ peut être indexé par le nombre entier $u = \sum_{i=1}^{m} u_i e_i$.

CHAPITRE 3

LES CARACTÈRES DE GROUPES FINIS COMMUTATIFS

3.1. Définitions

Soit G un groupe abélien fini dont on notera + l'opération.

Définition 3.1.1. — Un caractère χ du groupe G est un homomorphisme de G dans le groupe multiplicatif $\mathbf{U}$ des nombres complexes de module 1. C'est-à-dire que

$$\begin{cases} \chi(0) & = & 1 \\ \chi(a+b) & = & \chi(a)\chi(b). \end{cases}$$

Nous noterons $\widehat{G}$ l'ensemble des caractères du groupe G.

Remarques.

– Soit $n = \sharp G$ le nombre d'éléments de G. Nous savons que

$$\underbrace{a+a+a+...+a}_{n\ fois} = 0$$

donc

$$\chi(a)^n = 1$$

si bien que les valeurs prises par la fonction complexe χ sont des racines n^{e}de l'unité ;

– Il découle de la remarque précédente que $\widehat{G}$ est lui même un ensemble fini ;

– Il est aussi facile de voir que $\widehat{G}$ muni de la multiplication des fonctions complexes est un groupe abélien fini ;

3.2. Exemples

3.2.1. Les caractères de $\mathbf{Z}/n\mathbf{Z}$. — Pour tout u élément de $\mathbf{Z}/n\mathbf{Z}$ nous notons χ_u la fonction complexe définie sur $\mathbf{Z}/n\mathbf{Z}$ par

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

nous obtenons ainsi tous les caractères du groupe $\mathbf{Z}/n\mathbf{Z}$.

3.2.2. Les caractères de $\{0,1\}^m$. — Pour tout $u = (u_1, u_2, .., u_m)$ élément de $\{0,1\}^m$ nous notons χ_u la fonction complexe définie sur $\{0,1\}^m$ par

$$\chi_u(v) = (-1)^{<u,v>} = (-1)^{u_1v_1+u_2v_2+...+u_mv_m}$$

où $v = (v_1, v_2, ..., v_m)$. Nous obtenons ainsi tous les caractères du groupe $\{0,1\}^m$.

3.3. Quelques résultats

Théorème 3.3.1. — *Soit H un sous groupe d'un groupe abélien fini G, ψ un caractère de H. Alors ψ peut être prolongé en un caractère χ de G.*

Preuve. Supposons $H \neq G$. Soit a un élément de G qui n'est pas dans H et H_1 le sous groupe de G engendré par a et H. Notons m le plus petit entier tel que

$$\underbrace{a + a + a + ... + a}_{m\ fois} \in H$$

(ainsi m est l'ordre de a dans G/H).

Tout élément g de H_1 peut s'écrire de manière unique

$$g = \underbrace{a + a + a + ... + a}_{j\ fois} + h$$

où $0 \leq j < m$ et où $h \in H$.

Définissons ψ_1 sur H_1 par

$$\psi_1(g) = \omega^j \psi(h)$$

où ω est un complexe vérifiant

$$\omega^m = \psi(a^m)$$

alors ψ_1 est un caractère de H_1 qui prolonge ψ.

Théorème 3.3.2. — *Si g_1 et g_2 sont deux éléments distincts du groupe G il existe un caractère χ tel que $\chi(g_1) \neq \chi(g_2)$.*

Preuve. Il suffit de montrer que pour $h = g_1 - g_2 \neq 0$ il existe un caractère χ tel que $\chi(h) \neq 1$. pour cela considérons le groupe cyclique H engendré par h. Il est alors facile de construire un caractère ψ sur H tel que $\psi(h) \neq 1$. On prolonge ψ sur G tout entier en vertu du théorème précédent.

Théorème 3.3.3. — *Si χ est un caractère non trivial (c'est-à-dire qui n'est pas la fonction constante 1) du groupe abélien fini G alors*

$$\sum_{g \in G} \chi(g) = 0$$

et si g est un élément non nul de G alors

$$\sum_{\chi \in \widehat{G}} \chi(g) = 0.$$

Preuve. Puisque χ est non trivial il existe $h \in G$ tel que $\chi(h) \neq 1$. Alors

$$\chi(h) \sum_{g \in G} \chi(g) = \sum_{g \in G} \chi(g + h) = \sum_{g \in G} \chi(g)$$

donc

$$(\chi(h) - 1) \sum_{g \in G} \chi(g) = 0$$

d'où

$$\sum_{g \in G} \chi(g) = 0.$$

Soit $q(g)$ la fonction de $\widehat{G}$ dans $\mathbf{U}$ définie par

$$q(g)(\chi) = \chi(g)$$

c'est un caractère non trivial de $\widehat{G}$ en vertu du théorème 3.3.2. Par application de la première identité du théorème on obtient

$$\sum_{\chi \in \widehat{G}} q(g)(\chi) = 0$$

c'est-à-dire

$$\sum_{\chi\in\widehat{G}}\chi(g)=0.$$

Théorème 3.3.4. — *Le nombre d'éléments de $\widehat{G}$ est le même que celui de G.*

Preuve. En effet

$$\sharp\widehat{G}=\sum_{g\in G}\sum_{\chi\in\widehat{G}}\chi(g)$$

(Dans la somme sur $g\in G$ il n'y a qu'un terme non nul, celui obtenu pour $g=0$ et dans ce cas ce terme est bien $\sharp\widehat{G}$). Or

$$\sum_{g\in G}\sum_{\chi\in\widehat{G}}\chi(g)=\sum_{\chi\in\widehat{G}}\sum_{g\in G}\chi(g)=\sharp G.$$

Il est facile de vérifier que

Théorème 3.3.5. — *Soit q l'application de G dans $\widehat{\widehat{G}}$ définie par*

$$q(g)(\chi)=\chi(g)$$

q est un isomorphisme de groupes.

Remarquons aussi que dans chaque exemple nous avons pu trouver un isomorphisme entre G et $\widehat{G}$. Ceci peut se faire aussi dans le cas général.

En effet

$$G=\prod_{i=1}^{m}\mathbf{Z}/n_i\mathbf{Z}.$$

A tout élément $u=(u_1,u_2,...,u_m)$ de G associons le caractère χ_u défini par

$$\chi_u(v)=\prod_{k=1}^{m}e^{\frac{2i\pi u_k v_k}{n_k}}$$

on obtient ainsi un isomorphisme entre G et $\widehat{G}$ (et on a par la même occasion une description complète des caractères de G).

CHAPITRE 4

FONCTIONS COMPLEXES DÉFINIES SUR LES GROUPES ABÉLIENS FINIS. TRANSFORMATION DE FOURIER

Dans tout ce chapitre on suppose que G est un groupe abélien fini dont le nombre d'éléments est $\sharp G = n$. L'espace vectoriel des fonctions de G dans $\mathbf{C}$ est noté $\mathcal{F}(G)$.

4.1. Espace des fonctions sur un groupe abélien

Un élément de $\mathcal{F}(G)$ peut avoir plusieurs interprétations et par là même plusieurs notations. En effet une fonction $f \in \mathcal{F}(G)$ peut être définie par la donnée de ses images. Si les éléments de G ont pu être indexés sous la forme $g_1, g_2, ..., g_n$, notons $a_k = f(g_k)$. La fonction f peut alors être écrite sous la forme

$$f = (a_1, a_2, ..., a_n).$$

En fait cette écriture met l'accent sur les composantes de la fonction f dans une base particulière : la base $(e_i)_i$ où la fonction e_i est définie par

$$e_i(g_j) = \delta_{i,j} = \begin{cases} 1 & si \quad i = j \\ 0 & si \quad i \neq j. \end{cases}$$

Dans cette base en effet f s'écrit

$$f = \sum_{i=1}^{n} a_i e_i.$$

La fonction f peut aussi être considérée comme l'élément

$$P(X) = a_1 + a_2 X + ... + a_n X^{n-1}$$

de $\mathbf{C}[X]$.

L'espace $\mathcal{F}(G)$ est un espace vectoriel sur $\mathbf{C}$ de dimension n.

Sur cet espace nous pouvons définir le produit scalaire hermitien

$$< f_1, f_2 >= \frac{1}{n} \sum_{g \in G} f_1(g)\overline{f_2(g)}.$$

Théorème 4.1.1. — *Les caractères de G forment une base orthonormée de $\mathcal{F}(G)$.*

Preuve. En effet si $\chi_1 \neq \chi_2$

$$< \chi_1, \chi_2 >= \frac{1}{n} \sum_{g \in G} \chi_1(g)\overline{\chi_2(g)} = \frac{1}{n} \sum_{g \in G} \chi_1\overline{\chi_2}(g).$$

Mais $\chi_1\overline{\chi_2}$ est un caractère non trivial de G, en vertu du théoreme 3.3.3 $< \chi_1, \chi_2 >= 0$.

Il est facile de voir que $< \chi_1, \chi_1 >= 1$. Ceci permet de conclure.

4.2. Transformation de Fourier discrète

Soit f une fonction complexe définie sur G ($f \in \mathcal{F}(G)$). On peut décomposer f sur la base formée par les caractères de G :

$$f = \sum_{\chi \in \widehat{G}} \alpha_\chi \chi$$

posons

$$\widehat{f}(\chi) =< f, \chi >= \frac{1}{n} \sum_{a \in G} f(a)\overline{\chi(a)}$$

on a alors

$$\widehat{f}(\chi) = \sum_{\psi \in \widehat{G}} \alpha_\psi < \psi, \chi >= \alpha_\chi$$

et donc

$$f = \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\chi$$

Définition 4.2.1. — Le nombre $\widehat{f}(\chi)$ est la transformée de Fourier de f au point χ ;

la fonction $\widehat{f}$ de $\widehat{G}$ dans $\mathbf{C}$ est la transformée de Fourier de f ;

l'application T de $\mathcal{F}(G)$ dans $\mathcal{F}(\widehat{G})$ qui à f fait correspondre $\widehat{f}$ est l'opérateur de Fourier.

Théorème 4.2.2. — *L'opérateur de Fourier T de $\mathcal{F}(G)$ dans $\mathcal{F}(\widehat{G})$ est un isomorphisme d'espaces vectoriels.*

Preuve. T est une application linéaire. Elle est injective puisque si $f \neq 0$, alors f admet une composante non nulle dans la base formée par les caractères de G et cette composante est une valeur prise par la fonction $\widehat{f}$ ce qui prouve que $T(f) \neq 0$. Comme les deux espaces $\mathcal{F}(G)$ et $\mathcal{F}(\widehat{G})$ ont même dimension, T est bijective.

Nous allons établir quelques résultats sur les transformations de Fourier et en particulier calculer la norme de T. Pour cela nous serons amenés à chercher $\widehat{\widehat{f}}$ et nous rappelons à ce propos l'identification que l'on peut faire entre G et $\widehat{\widehat{G}}$ grâce à l'application q de G dans $\widehat{\widehat{G}}$ définie par

$$q(g)(\chi) = \chi(g).$$

Nous pouvons donc écrire

$$\widehat{\widehat{f}}\,(a) =< \widehat{f}, a >= \frac{1}{n} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\chi(a)}.$$

En remarquant que

$$\overline{\chi(a)} = \frac{1}{\chi(a)} = \chi(-a)$$

et en considérant la décomposition de f sur la base des caractères de G on voit que

Théorème 4.2.3. —

$$\widehat{\widehat{f}}\,(a) = \frac{1}{n} f(-a).$$

Remarquons que ce résultat nous permet de dire comment calculer la transformée de Fourier inverse.

Ecrivons maintenant la décomposition de $\widehat{f}$ sur la base des caractères de $\widehat{G}$ et pensons à l'identification de $\widehat{\widehat{G}}$ avec G

$$\widehat{f}(\chi) = \sum_{g \in G} \widehat{\widehat{f}}\,(g)\chi(g)$$

en utilisant le théorème de Pythagore et le théorème précédent

$$\|\widehat{f}\|^2 = \sum_{g\in G} |\widehat{\widehat{f}}(g)|^2$$

$$\|\widehat{f}\|^2 = \frac{1}{n^2}\sum_{g\in G} |f(-g)|^2$$

$$\|\widehat{f}\|^2 = \frac{1}{n}\|f\|^2.$$

On déduit de ces calculs les deux théorèmes suivants

Théorème 4.2.4. —

$$\|T(f)\|^2 = \frac{1}{n}\|f\|^2.$$

Théorème 4.2.5. —

$$\sum_{\chi\in\widehat{G}} |\widehat{f}(\chi)|^2 = \frac{1}{n}\sum_{g\in G} |f(g)|^2.$$

4.3. Calculs élémentaires

Sur $\mathcal{F}(G)$ il existe deux opérateurs de base importants car ils sont étroitement liés à la loi de groupe de G, ce sont les translations T_t définies par

$$T_t(f)(x) = f(x+t)$$

et la symétrie $^\vee$ définie par

$$\overset{\vee}{f}(x) = f(-x).$$

Attention $+$ est la loi du groupe G et $-x$ est l'opposé de x dans le groupe G ; donc si la loi est notée multiplicativement il faut en tenir compte dans l'écriture ! Par exemple si g est dans $\mathcal{F}(\widehat{G})$ alors $\overset{\vee}{g}(\chi) = f(\frac{1}{\chi})$. De même $T_\psi(g)(\chi) = g(\chi\psi)$.

La question qui se pose est de savoir comment se comportent ces opérateurs vis-à-vis de la transformation de Fourier.

Théorème 4.3.1. — *Soit f un élément de $\mathcal{F}(G)$. On dispose des égalités suivantes*

$$\widehat{T_t(f)}(\chi) = \chi(t)\widehat{f}(\chi)$$

$$\widehat{\overset{\vee}{f}}(\chi) = \overset{\vee}{\widehat{f}}(\chi)$$

Preuve. Il suffit dans les deux cas de revenir à la définition de la transformée de Fourier.

$$\widehat{T_t(f)}(\chi) = \frac{1}{n}\sum_{a\in G} T_t(f)(a)\overline{\chi(a)}$$

c'est-à-dire

$$\widehat{T_t(f)}(\chi) = \frac{1}{n}\sum_{a\in G} f(a+t)\overline{\chi(a)}$$

ou encore en posant $b = a + t$

$$\widehat{T_t(f)}(\chi) = \frac{1}{n}\sum_{b\in G} f(b)\overline{\chi(b)}\chi(t)$$

ce qui démontre la première égalité. On obtient la deuxième égalité par une démonstration analogue.

4.4. La convolution

Définition 4.4.1. — 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 4.4.2. — *La transformée de Fourier d'un produit de convolution est le produit (ordinaire) des transformées de Fourier*

$$\widehat{f_1 * f_2} = \widehat{f_1}\widehat{f_2}.$$

Preuve.

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

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

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

et la dernière expression correspond bien au produit de $\widehat{f_1}(\chi)$ par $\widehat{f_2}(\chi)$.

Il suffit de revenir à la définition pour voir que

Théorème 4.4.3. — *Le symétrique d'un produit de convolution est le produit de convolution des symétriques*

$$f_1 \overset{\vee}{*} f_2 = \overset{\vee}{f_1} * \overset{\vee}{f_2}.$$

En utilisant les résultats précédents on peut également vérifier que

Théorème 4.4.4. — *La transformée de Fourier d'un produit de fonctions est n fois le produit de convolution des transformées de Fourier*

$$\widehat{f_1 f_2} = n \widehat{f_1} * \widehat{f_2}.$$

4.5. Les filtres linéaires stationnaires

Soit H un opérateur linéaire de $\mathcal{F}(G)$ dans lui même qui commute avec les opérateurs de translation, c'est-à-dire que pour tout $t \in G$

$$H(T_t(f)) = T_t(H(f)).$$

On dit que dans ces conditions H est un filtre linéaire stationnaire. Nous avons vu dans le chapitre Introduction que les caractères χ sont des vecteurs propres de H associés respectivement aux valeurs propres $H(\chi)(0)$. Puisque les caractères forment une base de $\mathcal{F}(G)$ on dispose donc d'une décomposition en sous espaces propres de H. Dans la base des caractères la matrice d'un filtre linéaire stationnaire est une matrice diagonale ayant les valeurs $H(\chi)(0)$ sur la diagonale.

Nous allons voir que ces filtres peuvent être réalisés grâce à une convolution, plus précisément on dispose du théorème

Théorème 4.5.1. — *Soit H un filtre linéaire stationnaire sur $\mathcal{F}(G)$, alors il existe une fonction h appartenant à $\mathcal{F}(G)$ telle que pour toute fonction f appartenant à $\mathcal{F}(G)$ on ait*

$$H(f) = h * f.$$

Preuve. Définissons l'application Θ sur $\mathcal{F}(G)$ par

$$\Theta(f) = H(\overset{\vee}{f})(0).$$

Θ est une forme linéaire. Si on décompose f sous la forme

$$f = \sum_{u \in G} f(u) e_u$$

où $e_u(v) = \delta_{u,v}$ alors

$$\Theta(f) = \sum_{u \in G} f(u)\Theta(e_u)$$

et en définissant la fonction h par $h(u) = n\Theta(e_u)$ on obtient

$$\Theta(f) = \frac{1}{n} \sum_{u \in G} f(u)h(u)$$

ou encore

$$H(f)(0) = \frac{1}{n} \sum_{u \in G} f(-u)h(u)$$

c'est-à-dire

$$H(f)(0) = h * f(0).$$

En appliquant cette formule à la fonction $T_x(f)$ on obtient

$$H(T_x(f))(0) = h * T_x(f)(0) = h * f(x)$$

mais

$$H(T_x(f))(0) = T_x(H(f))(0) = H(f)(x)$$

donc

$$H(f)(x) = h * f(x).$$

CHAPITRE 5

QUELQUES EXEMPLES. FONCTIONS DE WALSH, DE RADEMACHER, DE HAAR

5.1. Transformation de Fourier sur $\mathbf{Z}/n\mathbf{Z}$

On se place donc dans le cas où $G = \mathbf{Z}/n\mathbf{Z}$. 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 entre 0 et $n-1$ si bien qu'une transformée de Fourier apparaît ici comme fonction d'un tel entier. Plus précisément si $f \in \mathcal{F}(G)$, notons $a_u = f(u)$ où $u = 0, 1, ..., n-1$. Dans ces conditions

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

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

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 $a_0, a_1, ..., a_{n-1}$, et h celle dont les images sont $b_0, b_1, ..., b_{n-1}$, notons

$$P_f(X) = \frac{1}{n}\Big(a_0 + a_1X + ... + a_{n-1}X^{n-1}\Big)$$

$$P_h(X) = \frac{1}{n}\Big(b_0 + b_1X + ... + b_{n-1}X^{n-1}\Big).$$

On sait que

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

donc

$$P_{f*h} = P_f P_h \quad mod\ (X^n - 1).$$

Remarquons en outre que

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

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.

5.2. Transformation de Fourier sur $(\mathbf{Z}/n\mathbf{Z})^m$

Dans ce cas G est le groupe produit $(\mathbf{Z}/n\mathbf{Z})^m$. Soit f une fonction complexe définie sur G, notons pour tout élément $u = (u_1, u_2, ..., u_m)$ de G

$$a_{u_1 u_2 ... u_m} = f(u)$$

et

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

On sait que les caractères de G sont indexés par les éléments de G et on peut écrire

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

c'est-à-dire encore

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

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

$$P_{f*h}(X_1, X_2, ..., X_m) = P_f(X_1, X_2, ..., X_m)P_h(X_1, X_2, ..., X_m) \quad mod\ (\mathcal{I}).$$

5.3. Transformation d'Hadamard

La transformation d'Hadamard relève du cas particulier où $G = (\mathbf{Z}/2\mathbf{Z})^m$. Dans ce cas là 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 $x = (x_1, x_2, ..., x_m) \in G$ représente le nombre entier compris entre 0 et $2^m - 1$

$$x_1 + 2x_2 + ... + 2^{m-1}x_m.$$

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

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

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

$$W_\lambda = \prod_{j=1}^{n} {r'}_j$$

où

$${r'}_j = \begin{cases} r_j & si \quad \lambda_j = 1 \\ 1 & si \quad \lambda_j = 0. \end{cases}$$

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

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

et

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

A partir des fonctions de Rademacher on peut définir une autre base orthonormée intéressante : les fonctions de Haar. Nous renvoyons le lecteur à l'article suivant (en annexe) : Computing with discrete Haar functions (preprint de l'équipe ATI).

CHAPITRE 6

LE CALCUL DES DIVERSES TRANSFORMATIONS

6.1. Transformation 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 $\mathbf{Z}/n\mathbf{Z}$. 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

$$(W_8^3)^2 = (W_8^7)^2 = W_4^3$$
$$W_8^3 = -W_8^7.$$

On rappelle que si

$$f = (a_0, a_1, ..., a_{2^m-1})$$

et si

$$P_f(X) = \frac{1}{2^m}\Big(a_0 + a_1X + ... + a_{2^m-1}X^{2^m-1}\Big)$$

alors

$$\widehat{f}(u) = \widehat{a_u} = P_f(W_{2^m}^u).$$

Pour tout polynôme

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

notons

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

et

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

alors

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

ce qui donne si $0 \leq k \leq 2^{r-1} - 1$

$$P(W_{2^r}^k) = P_0(W_{2^{r-1}}^k) + W_{2^r}^k P_1(W_{2^{r-1}}^k)$$

et

$$P(W_{2^r}^{k+2^{r-1}}) = P_0(W_{2^{r-1}}^k) - W_{2^r}^k P_1(W_{2^{r-1}}^k).$$

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

Remarquons tout d'abord que si on a tabulé les valeurs de $W_{2^m}^k$ alors on dispose aussi des valeurs de $W_{2^r}^k$ pour tout $r \leq m$.

W_8^0	W_8^1	W_8^2	W_8^3	W_8^4 $-W_8^0$	W_8^5 $-W_8^1$	W_8^6 $-W_8^2$	W_8^7 $-W_8^3$
W_4^0		W_4^1		W_4^2 $-W_4^0$		W_4^3 $-W_4^1$	
W_2^0				W_2^1 $-W_2^0$			

Pratique du calcul. Le coefficient $\frac{1}{n}$ n'interviendra qu'à la fin. Pour cela au lieu de calculer avec le polynôme P_f nous calculerons avec $P = nP_f = a_0 + ... + a_{2^m-1}X^{2^m-1}$.

L'exemple $m = 3$ est suffisamment instructif pour décrire l'algorithme. Remarquons que

$$P_{000}(X) = a_0, P_{001}(X) = a_4, P_{010}(X) = a_2, P_{011}(X) = a_6$$
$$P_{100}(X) = a_1, P_{101}(X) = a_5, P_{110}(X) = a_3, P_{111}(X) = a_7.$$

On commence donc à faire une permutation σ des éléments

$$a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7$$

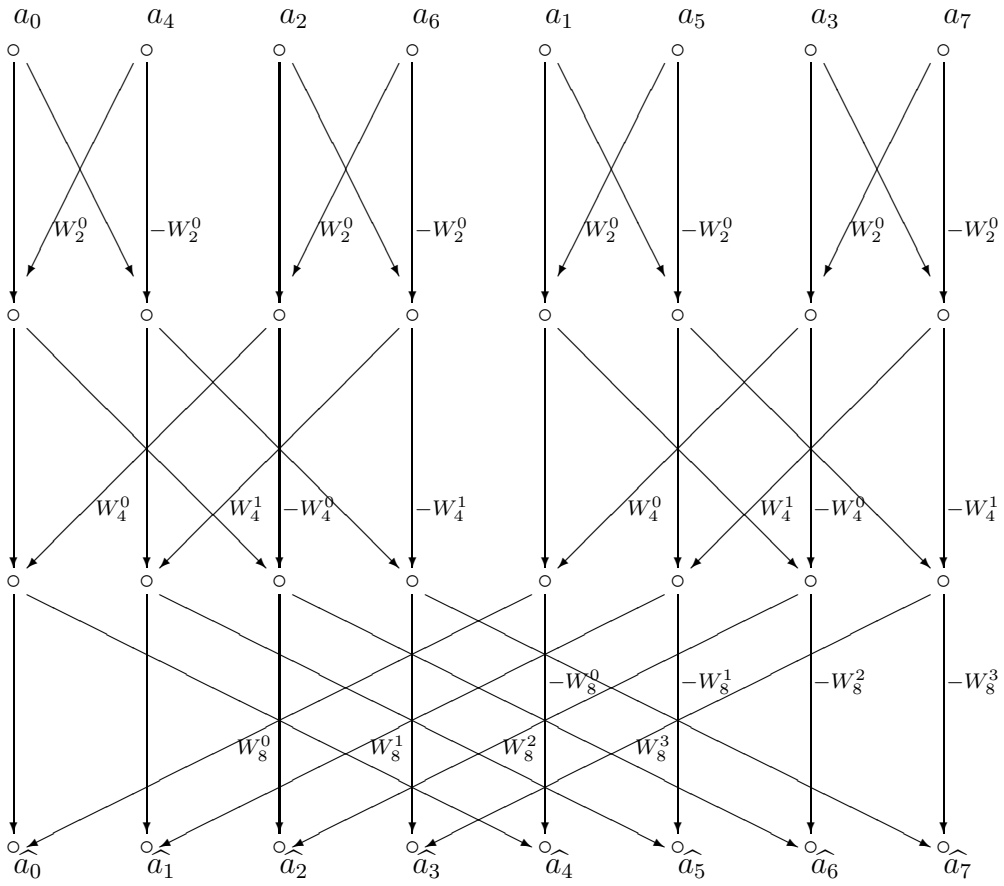

FIGURE 1. La FFT sur 8 points

pour les mettre dans l'ordre

$$a_0, a_4, a_2, a_6, a_5, a_3, a_7.$$

Ceci se fait facilement en remarquant qu'à chaque indice supposé écrit en binaire on fait correspondre l'indice obtenu en écrivant les bits dans l'ordre inverse. Ainsi l'indice $4 = 100$ est transformé en $1 = 001$. la suite du calcul de la transformée de Fourier se fait en trois étapes indiquées par la figure 1 et à la fin on divise les coefficient obtenus par 8.

Appelons M_8^1, M_8^2, M_8^3 les matrices

$$M_8^1 = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$M_8^2 = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}$$

$$M_8^3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \end{pmatrix}$$

S_1, S_2, S_3 les matrices diagonales définies par

$$S_1 = Diag(1, W_2^0, 1, W_2^0, 1, W_2^0, 1, W_2^0)$$

$$S_2 = Diag(1, 1, W_4^0, W_4^1, 1, 1, W_4^0, W_4^1)$$

$$S_3 = Diag(1, 1, 1, 1, W_8^0, W_8^1, W_8^2, W_8^3)$$

et enfin Σ la matrice de la permutation "reverse bit" σ.

Dans ces conditions la matrice F_8 de la transformation de Fourier sur 8 points s'écrit

$$F_8 = \frac{1}{8} M_8^3 S_3 M_8^2 S_2 M_8^1 S_1 \Sigma.$$

Ceci se généralise facilement pour $n = 2^m$. Le nombre d'opérations à effectuer pour calculer cette transformation est de l'ordre de $nlog(n)$.

6.2. Transformation d'Hadamard rapide

Le calcul ici peut être mené de façon tout à fait analogue au calcul du paragraphe précédent.

Soit f une fonction définie sur le groupe $G = \{0,1\}^m$ à valeurs complexes. Notons alors conformément au système d'indexation des éléments de G que nous avons déjà expliqué (ici interprétation des éléments de G comme développements binaires de nombres) $a_i = f(i)$.

Là encore nous calculerons la transformée au coefficient $\frac{1}{2^m}$ près. Si bien que nous avons en fait à évaluer des sommes du type

$$P(x) = \sum_{y=0}^{2^r-1} a_y (-1)^{<x,y>}$$

où $x = (x_1, x_2, ..., x_r)$ et $y = (y_1, y_2, ..., y_r)$. Définissons alors

$$P_0(u) = \sum_{v=0}^{2^{r-1}-1} a_u (-1)^{<u,v>}$$

et

$$P_1(u) = \sum_{v=0}^{2^{r-1}-1} a_{u+2^{r-1}} (-1)^{<u,v>}$$

où $u = (u_1, u_2, ..., u_{r-1})$ et $v = (v_1, v_2, ..., v_{r-1})$. On peut alors écrire

$$P(x) = P_0(\tau(x)) + (-1)^{x_r} P_1(\tau(x))$$

où $\tau(x) = (x_1, x_2, ..., x_{r-1})$. Ceci donne une relation tout à fait comparable à celle obtenue dans le cas du paragraphe précédent.

Prenons là aussi le cas $n = 2^3 = 8$. Remarquons qu'on obtient

$$P_{000}(X) = a_0, P_{001}(X) = a_1, P_{010}(X) = a_2, P_{011}(X) = a_3$$
$$P_{100}(X) = a_4, P_{101}(X) = a_5, P_{110}(X) = a_6, P_{111}(X) = a_7$$

si bien que la transformée se fait conformément à la figure 2.

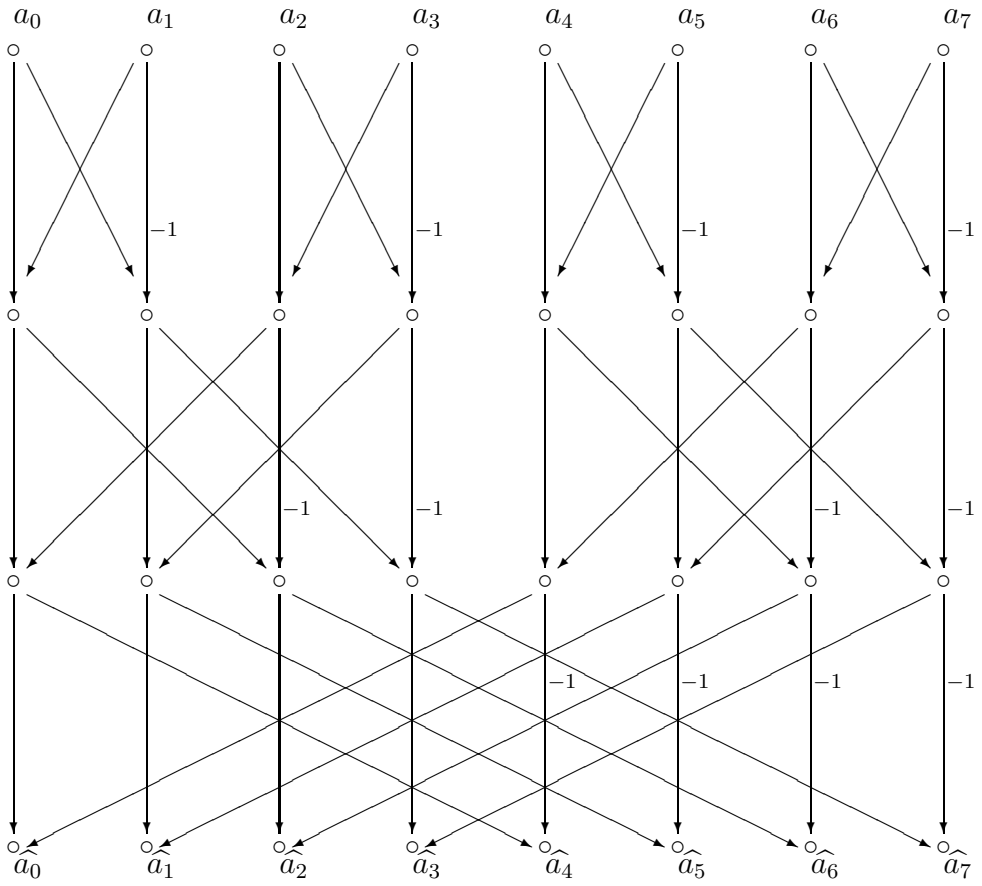

FIGURE 2. La FHT sur 8 points

Reprenons les matrices M_8^1, M_8^2, M_8^3 définies dans le paragraphe précedent.

La matrice T_8 de la transformation d'Hadamard sur 8 points s'écrit

$$T_8 = \frac{1}{8} M_8^3 M_8^2 M_8^1.$$

Ceci se généralise facilement pour $n = 2^m$. Le nombre d'opérations à effectuer pour calculer cette transformation est de l'ordre de $nlog(n)$.

Remarques. Les matrice T_{2^m} des transformations d'Hadamard sont au facteur 2^m près les matrices H_{2^m} d'Hadamard définies par

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

et

$$H_{2^m} = H_2 \bigotimes H_{2^{m-1}}$$

où $A \bigotimes B$ représente le produit de Kronecker de deux matrices A et B, c'est-à-dire la matrice obtenu en remplaçant dans la matrice A chaque coefficient a par le bloc matriciel aB.

Par exemple

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

Ces matrices vérifient la relation

$$HH^t = 2^m I.$$

Il est facile de retrouver à partir des propriétés des produits de Kronecker la décomposition de H_{2^m} sous la forme déjà indiquée

$$H_{2^m} = M_{2^m}^m ... M_{2^m}^1$$

on peut pour cela commencer par démontrer que

$$M_{2^m}^i = I_{2^{m-i}} \bigotimes H_2 \bigotimes I_{2^{i-1}}$$

pour $1 \leq i \leq m$.

CHAPITRE 7

FONCTIONS À VALEURS DANS UN CORPS FINI. TRANSFORMATION DE MATTSON-SOLOMON

7.1. Position du problème

Soit G le groupe abélien fini $\mathbf{Z}/n\mathbf{Z}$. Etant donné $q = p^s$ une puissance d'un nombre premier p notons $\mathbf{F}_q$ le corps à q éléments. Nous voulons étudier les fonctions de G dans $\mathbf{F}_q$. Pour cela nous allons introduire l'équivalent de la transformation de Fourier, où le groupe multiplicatif des nombres complexes de module 1 est remplacé par le groupe multiplicatif d'un corps fini (privé du zéro). Pour rendre ceci possible il convient de construire un corps fini $\mathbf{F}_{q^m}$ qui contienne à la fois le corps $\mathbf{F}_q$ et un sous groupe multiplicatif de $\mathbf{F}_{q^m}^*$ d'ordre n. Ceci n'est possible que si n est premier avec q (donc avec p).

Nous supposerons désormais que n est premier avec p. Il existe alors un plus petit entier m tel que n divise $q^m - 1$. Les zéros de $x^n - 1$ forment un sous groupe cyclique de $\mathbf{F}_{q^m}^*$. Nous noterons α un générateur de ce sous groupe.

Nous allons étudier maintenant les fonctions définies sur G et à valeurs dans $\mathbf{F}_{q^m}$ et comme cas particuliers, si nous voulons, les fonctions de G dans $\mathbf{F}_q$.

Définissons pour tout $0 \leq i \leq n-1$ la fonction ψ_i par

$$\psi_i(j) = \alpha^{ij}.$$

On vérifie que

$$\begin{cases} \psi_i(0) & = & 1 \\ \psi_i(a+b) & = & \psi_i(a)\psi_i(b). \end{cases}$$

Ces fonctions jouent donc le rôle des caractères.

Définition 7.1.1. — Soit $f = (a_0, ..., a_{n-1})$ une fonction définie sur G à valeurs dans $\mathbf{F}_{q^m}$. La transformée de Mattson Solomon de f est la fonction $\widehat{f} = (\widehat{a_0}, ..., \widehat{a_{n-1}})$ où

$$\widehat{a_j} = \frac{1}{(n \ mod \ p)} \sum_{i=0}^{n-1} a_i \alpha^{(n-j)i}.$$

Si on considére là encore le polyôme $P_f(X) = \frac{1}{(n \ mod \ p)}(a_0 + a_1 X + ... + a_{n-1} X^{n-1})$ associé à la fonction$f$, on constate que

$$\widehat{a_j} = P_f(\alpha^{n-j}).$$

Théorème 7.1.2. — *Soit f une fonction de G dans $\mathbf{F}_{q^m}$. La double transformée de Mattson Solomon de f vérifie*

$$\widehat{\widehat{f}}\,(i) = \frac{1}{(n \ mod \ p)} a_{n-i}.$$

Preuve. En revenant à la définition de la transformée de Mattson solomon on obtient

$$\widehat{\widehat{f}}\,(i) = \frac{1}{(n \ mod \ p)} \sum_{j=0}^{n-1} \widehat{f}(j) \alpha^{j(n-i)}$$

soit

$$\widehat{\widehat{f}}\,(i) = \frac{1}{(n \ mod \ p)^2} \sum_{j=0}^{n-1} \sum_{l=0}^{n-1} a_l \alpha^{l(n-j)} \alpha^{j(n-i)}$$

ou encore

$$\widehat{\widehat{f}}\,(i) = \frac{1}{(n \ mod \ p)^2} \sum_{l=0}^{n-1} a_l \sum_{j=0}^{n-1} (\alpha^{-(l+i)})^j$$

ce qui donne le résultat attendu.

En particulier cette formule nous permet de voir comment est réalisée la transformation inverse

$$f(i) = (n \ mod \ p) P_{\widehat{f}}(\alpha_i)$$

7.2. Un exemple

Soit $n = 2^4 - 1$, $G = \mathbf{Z}/n\mathbf{Z}$ et f la fonction de G dans $\{0, 1\}$ définie par

$f(0) = 1,\ f(1) = 0,\ f(2) = 0,\ f(3) = 0,\ f(4) = 1,\ f(5) = 1,\ f(6) = 1,\ f(7) = 1,$
$f(8) = 0,\ f(9) = 1,\ f(10) = 0,\ f(11) = 1,\ f(12) = 1,\ f(13) = 0,\ f(14) = 0.$

Montrer qu'il existe un polynôme P à coefficients dans $\mathbf{F}_{16}$ tel que $f(i) = P(\alpha_i)$ pour tout i. Calculer ce polynôme.

Ici nous avons $n = 15$ et $p = 2$, ce qui donne $n \ mod \ p = 1$. Donc pour tout i

$$f(i) = P_{\widehat{f}}(\alpha_i)$$

ce qui veut dire que le polynôme que nous cherchons est le polynôme associé à la transformée de Mattson Solomon de f. Le calcul de cette transformée fournit

$$P(X) = \alpha^3 X^{14} + \alpha^6 X^{13} + \alpha^{12} X^{11} + \alpha^9 X^7.$$

Remarques. La fonction f que nous avons étudiée ne prend que les valeurs 0 et 1, on peut donc tout aussi bien considérer que cette fonction est à valeurs complexes et utiliser sa transformation de Fourier. Dans ce cas on peut écrire

$$f(v) = n P_{\widehat{f}}(e^{\frac{2i\pi v}{n}})$$

et donc il existe un polynôme P à coefficients complexes tel que pour tout v on ait

$$f(v) = P(e^{\frac{2i\pi v}{n}}).$$

CHAPITRE 8

APPROXIMATION DE FONCTIONS RÉELLES PAR DES FONCTIONS DISCRÈTES. APPLICATIONS À DES PROBLÈMES DE FILTRAGE

Parmi les diverses et nombreuses applications de la transformée de Fourier discrète, il y en a au moins deux qui sont fondamentales : le calcul des coefficients de Fourier d'une fonction périodique et le calcul de la transformée de Fourier d'une fonction d'une variable réelle. En effet ces deux situations permettent non seulement un calcul, mais éclairent les liens qui existent entre ces divers cas.

8.1. Les séries de Fourier

Soit f une fonction d'une variable réelle périodique de période T. Nous supposerons que f est développable en série de Fourier sous la forme

$$f(t) = \sum_{k=-\infty}^{+\infty} c_k(f) e^{2i\pi k \frac{t}{T}}$$

les coefficients $c_k(f)$ étant donnés par

$$c_k(f) = \frac{1}{T} \int_0^T f(t) e^{-2i\pi k \frac{t}{T}} dt.$$

Il nous faut calculer les coefficients $c_k(f)$. Pour cela on peut avoir deux idées suggérées par les deux formules précédentes. La première formule nous suggère d'interpoler la fonction f en un certain nombre de points par un polynôme trigonométrique, les coefficients de ce polynôme étant pris alors comme approximations des coefficients correspondants de la série de Fourier. La deuxième formule quant à elle nous incite à calculer l'intégrale du second membre par une méthode approchée. Dans les deux cas nous

allons échantillonner le segment $[0, T]$ en N intervalle de longueur ΔT. Nous avons donc

$$N.\Delta T = T$$

et nous définirons la fréquence d'échantillonnage par

$$F = \frac{1}{\Delta T}.$$

Les points de l'échantillonnage sont les points

$$t_s = s.\Delta T.$$

En ces points la fonction f prend les valeurs

$$f(t_s) = \sum_{k=-\infty}^{+\infty} c_k(f) e^{2i\pi k \frac{s\Delta T}{T}}$$

ou encore

$$f(t_s) = \sum_{k=-\infty}^{+\infty} c_k(f) e^{2i\pi ks/N}.$$

Si nous voulons interpoler f aux points $t_s \quad s = 0, 1, .., N-1$ par un polynôme trigonométrique, nous pouvons appliquer ce que nous savons sur la transformée de Fourier discrète. Ainsi nous pourons écrire

$$f(t_s) = \sum_{k=0}^{N-1} C_k(f) e^{2i\pi ks/N}$$

où les coefficients $C_k(f)$ sont obtenus par transformation de Fourier discrète

$$C_k(f) = \frac{1}{N} \sum_{s=0}^{N-1} f(t_s) e^{-2i\pi ks/N}.$$

On remarque en passant que cette dernière formule n'est rien d'autre que l'approximation par la méthode des rectangles de l'intégrale qui donne le véritable coefficient de Fourier. On rejoint donc la deuxième idée dont nous parlions précédemment.

Remarquons que dans l'espace des temps nous avons une période T que nous avons échantillonné grâce à un découpage en N segments de longueur ΔT, ce qui nous donne une fréquence d'échantillonnage $F = 1/\Delta T$. L'espace des fréquences est échantillonné grâce à N intervalles de longueur $\Delta F = 1/T$ ce qui nous donne une étendue de $N.\Delta F = F$ pour

l'espace des fréquences et une fréquence d'échantillonnage de l'espace des fréquences de T. En résumé nous disposons des relations

$$T = N.\Delta T$$

$$F = N.\Delta F$$

$$F = 1/\Delta T$$

$$T = 1/\Delta F$$

$$TF = N.$$

Le problème qui se pose maintenant et de comparer le coefficient calculé $C_k(f)$ avec le véritable coefficient $c_k(f)$. Pour cela repartons de la formule

$$f(t_s) = \sum_{k=-\infty}^{+\infty} c_k(f) e^{2i\pi ks/N}$$

qui en tenant compte de la périodicité s'écrit en supposant que la suite des coefficients de Fourier est sommable (ce qui est le cas si f est suffisamment régulière)

$$f(t_s) = \sum_{k=0}^{N-1} (\sum_{r=-\infty}^{+\infty} c_{k+rN}(f)) e^{2i\pi ks/N}$$

En comparant cette expression avec celle obtenue par interpolation et en vertu de l'unicité du polynôme trigonométrique d'interpolation de degré $N-1$ on obtient

$$C_k(f) = \sum_{r=-\infty}^{+\infty} c_{k+rN}(f)$$

ou encore

$$c_k(f) = C_k(f) - \sum_{r\neq 0} c_{k+rN}(f).$$

L'approximation sera donc accepable si les coefficients de Fourier décroissent rapidement, ce qui est le cas si la fonction f est très régulière. Autrement dit l'approximation sera bonne si les hautes fréquences sont quasi absentes du signal. Bien entendu si le signal est lui même un

polynôme trigonométrique de degré inférieur ou égal à $N-1$, les c_k et les C_k coincident (la formule d'approximation donne une valeur exacte).

Considérons un signal périodique de spectre borné (c'est-à-dire un polynôme trigonométrique). Suposons le spectre inclus dans l'intervalle $[-S/2, S/2]$. Alors le calcul envisagé est exact si le signal est échantilloné avec une fréquence F au moins égale à S.

Le lecteur pourra méditer sur l'inconvénient qui résulte de la non application de cette règle avec le contre exemple suivant :

On considère les deux fonctions $cos(2\pi t)$ et $cos(18\pi t)$. On constate que ces deux fonctions coincident pour les valeurs $t = k/8$ (ce phénomène est appelé l'aliasing).

8.2. La transformation de Fourier sur R

Soit f une fonction d'une variable rélle et on suppose qu'on peut écrire

$$a(f)(\nu) = \int_{\infty}^{+\infty} f(t)e^{-2i\pi\nu t}dt$$

et

$$f(t) = \int_{-\infty}^{+\infty} a(f)(\nu)e^{2i\pi\nu t}d\nu.$$

Nous cherchons à calculer la transformée de Fourier $a(f)(\nu)$; ceci ne pourra bien entendu se faire que pour un échantillonnage fini de valeurs de ν. Une idée est de fixer une période de temps T et d'échantillonner la fonction en des points $t_s = s.\Delta T$. On posera encore $F = 1/\Delta T$. On peut alors écrire

$$f(t_s) = \int_{-\infty}^{+\infty} a(f)(\nu)e^{2i\pi\nu s/F}d\nu$$

ou encore

$$f(t_s) = \sum_{k=-\infty}^{+\infty} \int_{kF}^{(k+1)F} a(f)(\nu)e^{2i\pi\nu s/F}d\nu$$

et sous réserve de convergence, en posant

$$A(f)(\nu) = \sum_{k=-\infty}^{+\infty} a(f)(\nu + kF)$$

on obtient

$$f(t_s) = \int_0^F A(f)(\nu) e^{2i\pi\nu s/F} d\nu.$$

Il est alors facile de remarquer que la fonction $A(f)(\nu)$ est périodique de de période F, et qu'on peut donc écrire son développement en série de Fourier (en supposant que la fonction soit développable en série de Fourier) sous la forme

$$A(f)(\nu) = \frac{1}{F} \sum_{s=-\infty}^{+\infty} f(t_s) e^{-2i\pi\nu s/F}.$$

Calculons alors $A(f)(\nu)$ aux divers points $\nu_k = k\Delta F$. On obtient

$$A(f)(\nu_k) = \frac{1}{F} \sum_{s=-\infty}^{+\infty} f(s\Delta T) e^{-2i\pi ks/N}.$$

Posons aussi

$$\Phi(t) = \sum_{s=-\infty}^{+\infty} f(t + sT)$$

on obtient alors

$$A(f)(\nu_k) = \frac{1}{F} \sum_{s=0}^{N-1} \Phi(t_s) e^{-2i\pi ks/N}.$$

On reconnait là une transformée de Fourier discrète dont l'inverse nous donne

$$\Phi(t_s) = \frac{1}{T} \sum_{k=0}^{N-1} A(f)(\nu_k) e^{2i\pi ks/N}.$$

En conséquence pour calculer une valeur approchée de $a(f)(\nu_k)$ on peut penser à calculer $A(f)(\nu_k)$, qui sera lui même calculé de manière approchée par l'expression

$$B(f)(\nu_k) = \frac{1}{F} \sum_{s=0}^{N-1} f(t_s) e^{-2i\pi ks/N}.$$

Il est clair que si on a un signal $f(t)$ dont le spectre (c'est a dire la fonction $a(f)(\nu)$) est inclus dans le segment $[-\nu_c, \nu_c]$ (un tel signal est dit à bande limitée) et si la fréquence d'échantillonnage choisie F est supérieure à $2\nu_c$, alors la fonction périodique $A(f)(\nu)$ est égale à $a(f)(\nu)$ sur le segment $[-F/2, F/2]$. Evidemment à l'extérieur de ce segment les deux fonctions diffèrent puisque $A(f)$ est prolongée par périodicité alors que $a(f)$ est nulle.

TABLE DES MATIÈRES