Transformation de Fourier discrète

Le paragraphe 13.6 du programme de l'Agrégation s'intitule « Transformée de Fourier » et contient les thèmes : Transformée de Fourier discrète sur un groupe abélien fini. Transformée de Fourier rapide. Nous allons motiver l'utilisation de la transformée de Fourier discrète par le problème de la multiplication de (grands) polynômes, puis décrire l'algorithme FFT qui est la raison de l'efficacité de la méthode, puis enfin revenir sur la dénomination « Transformée de Fourier ».

1 Multiplication de polynômes sur machine

Soit K un corps. Dans les applications, on est intéressé par les corps $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$ ([1]). En machine, on utilise en général l'une des deux représentations pour les polynômes :

- dense : $P = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$ est représenté par $[a_0, \dots, a_n]$,
- creuse : $P = \sum_{i=0}^{d} a_i x^{e_i}$, $e_0 < \cdots < e_d$, $a_i \neq 0$, est représenté par $[e_0, a_0, \dots, e_d, a_d]$.

Dans la suite, travaillons avec la représentation dense. Nous voulons additionner et multiplier les polynômes de manière efficace. Le coût est mesuré par le nombre d'opérations à effectuer dans le corps de coefficients K. Si on veut additionner deux polynômes P et Q de degré $< n$, la méthode naïve coefficient par coefficient requiert n additions. Si on veut les multiplier, le calcul de chaque coefficient $c_k = \sum_{i+j} a_i b_j$ nécessite n multiplications puis n additions, soit un coût total de $2n^2$ (le calcul précis tenant compte des effets de bord avec les indices fournit la même asymptotique en $2n^2$). C'est donc quadratique. L'enjeu est de réduire ce coût.

La transformation de Fourier discrète permet de faire bien mieux. L'idée est en quelque sorte de passer à une troisième représentation des polynômes, précisément la représentation par leurs valeurs sur un n-uplet de points. En effet, l'interpolation de Lagrange nous dit qu'un polynôme P de degré $< n$ est déterminé de manière unique par les valeurs $P(a_1), \dots, P(a_n)$ si les $a_i \in K$ sont tous distincts. Lorsque le corps K contient les racines n-èmes de l'unité $1, \zeta, \dots, \zeta^{n-1}$, le choix des valeurs $a_i = \zeta^i$ permet de mettre en place un algorithme récursif qui mène à une grande efficacité. Le lien avec la transformation de Fourier sur le groupe $G = \mathbb{Z}/n\mathbb{Z}$ s'explique par le fait que le groupe $\widehat{G} = \{1, \zeta, \dots, \zeta^{n-1}\}$ est le groupe dual de G, et nous y reviendrons.

1.1 Remarque. Pour être plus précis, l'expression « le corps K contient les racines n-èmes de l'unité » signifie que le cardinal de l'ensemble $\mu_n(K) := \{x \in K, x^n = 1\}$ est égal à n. On sait que $|\mu_n(K)| \leqslant n$ car le polynôme $X^n - 1 \in K[X]$ a au plus n racines. On ne peut avoir $|\mu_n(K)| = n$ que si n est premier avec la caractéristique $p \geqslant 0$ de K (condition vide si $p = 0$). En effet, si $p > 0$ et $n = pm$ est multiple de p, l'égalité $x^n = 1$ implique $(x^m - 1)^p = 0$ donc $x^m = 1$ si bien que $\mu_n(K) \subset \mu_m(K)$ dont le cardinal est au plus m.

1. Les corps $\mathbb{Q}$ et $\mathbb{F}_q$ sont plus propices à une implémentation machine que les corps $\mathbb{R}$ et $\mathbb{C}$ dont les éléments sont intrinsèquement complexes.

2 Transformation de Fourier discrète et algorithme FFT

On fixe un corps K contenant n racines n-èmes de l'unité. On rappelle que, comme tout sous-groupe fini du groupe multiplicatif d'un corps (commutatif), le groupe $\mu_n(K)$ est cyclique. On note $\mu_n^*(K)$ l'ensemble des racines primitives n-èmes de l'unité, qui sont les générateurs de $\mu_n(K)$.

2.1 Remarque. Sur un corps qui ne contient pas assez de racines de l'unité, on peut tout de même définir une transformation de Fourier discrète et un algorithme FFT en se plaçant sur un anneau plus grand $A = K[X]/(X^n + 1)$ obtenu en ajoutant des racines de l'unité. Cet anneau n'est pas nécessairement un corps, ni même intègre, et c'est pourquoi il est utile de présenter l'algorithme FFT sur un anneau effectif général. Dans ce texte, nous restons avec un corps K pour simplifier.

Fixons une racine primitive n-ème de l'unité ω. Pour tout polynôme $K \in K[X]$ qui est multiple de $X^n - 1$, les valeurs $F(\omega^i)$ sont nulles. On peut donc définir l'application *transformation de Fourier discrète* :

$$\mathsf{DFT}_\omega : K[X]/(X^n - 1) \to K^n \quad , \quad F \mapsto \ (F(1), F(\omega), \ldots, F(\omega^{n-1})).$$

C'est un morphisme de K-algèbres, lorsqu'on voit le but K^n comme l'algèbre produit où la multiplication se fait composante par composante. Son calcul rapide est effectué par un algorithme de type « diviser pour régner ». Pour appliquer cette idée, supposons que n est pair, $n = 2k$. Alors, $\omega^k = -1$ puisque $(\omega^k - 1)(\omega^k + 1) = \omega^n - 1 = 0$ et le premier facteur est différent de 0. On peut écrire deux divisions euclidiennes :

$$F = (X^k - 1)Q_0 + R_0 \ , \quad F = (X^k + 1)Q_1 + R_1 \quad \text{avec} \quad \deg R_0, \deg R_1 < k.$$

Ces écritures vont nous permettre le calcul de F sur les puissances paires et impaires de ω. En effet,

$$\begin{aligned} &\text{si } \ell \text{ est pair, } \omega^{k\ell} = 1 \text{ donc } F(\omega^\ell) = R_0(\omega^\ell), \\ &\text{si } \ell \text{ est impair, } \omega^{k\ell} = -1 \text{ et } F(\omega^\ell) = R_1(\omega^\ell). \end{aligned}$$

Outre l'application récursive, le point crucial qui est la source de l'efficacité de l'algorithme FFT et qui conduit au choix de racines primitives de l'unité est que le calcul de R_0 et R_1 est très simple. On le voit dans l'étape 2 de l'algorithme que nous présentons maintenant.

Entrée $\mathrm{F} = f_0 + \cdots + f_{n-1}\mathrm{X}^{n-1}$; les puissances $1, \omega, \cdots, \omega^{n-1}$ d'une racine n-ième principale de l'unité ω, n étant une puissance de 2.

Sortie $\mathrm{F}(1), \ldots, \mathrm{F}(\omega^{n-1})$.

1. Si $n = 1$, renvoyer f_0.
2. Sinon, soit $k = n/2$. Calculer

$$\mathrm{R}_0(\mathrm{X}) = \sum_{j=0}^{k-1} (f_j + f_{j+k})\mathrm{X}^j,$$

$$\bar{\mathrm{R}}_1(\mathrm{X}) = \mathrm{R}_1(\omega\mathrm{X}) = \sum_{j=0}^{k-1} (f_j - f_{j+k})\omega^j\mathrm{X}^j.$$

3. Calculer récursivement $\mathrm{R}_0(1), \mathrm{R}_0(\omega^2), \ldots, \mathrm{R}_0\big((\omega^2)^{k-1}\big)$ et $\bar{\mathrm{R}}_1(1), \bar{\mathrm{R}}_1(\omega^2), \ldots, \bar{\mathrm{R}}_1\big((\omega^2)^{k-1}\big)$.
4. Renvoyer $\mathrm{R}_0(1), \bar{\mathrm{R}}_1(1), \mathrm{R}_0(\omega^2), \bar{\mathrm{R}}_1(\omega^2), \ldots, \mathrm{R}_0\big((\omega^2)^{k-1}\big), \bar{\mathrm{R}}_1\big((\omega^2)^{k-1}\big)$.

2.2 Théorème. *Supposons que n est une puissance de 2. L'algorithme FFT requiert au plus $\frac{3n}{2}\log n$ opérations dans K.*

Preuve : Les puissances de ω sont connues donc ne coûtent rien. Le coût de l'appel en degré n est d'au plus $2 \times n/2$ additions et soustractions (pour le calcul de R_0 et R_1) et de $n/2$ multiplications (pour le calcul de $\bar{R}_1$), plus deux appels récursifs en degré $n/2$. La complexité $C(n)$ satisfait donc à la récurrence :

$$C(n) \leqslant \frac{3n}{2} + 2C(n/2).$$

En posant $D(m) = C(2^m)$ on obtient $D(m) \leqslant 3 \cdot 2^{m-1} + 2D(m-1)$ puis par récurrence :

$$D(m) \leqslant 3i2^{m-1} + 2^i D(m-i) \quad \text{pour tout } i \leqslant m.$$

Pour $i = m$ on obtient $D(m) \leqslant 3k2^{m-1}$ puisque $D(0) = 0$. En repassant à $n = 2^m$ i.e. $m = \log_2 n$ on obtient $C(n) \leqslant \frac{3n}{2}\log n$ comme annoncé. □

Nous démontrons maintenant que le morphisme $\mathsf{DFT}_\omega : K[X]/(X^n - 1) \to K^n$ est un isomorphisme et que dans des bases convenables, son inverse, l'interpolation, n'est rien d'autre que l'application $\mathsf{DFT}_{\omega^{-1}}$ à un facteur $\frac{1}{n}$ près. On rappelle que n est inversible dans K, cf remarque 1.1.

2.2.1 Proposition. *L'application $\mathsf{DFT}_\omega : K[X]/(X^n-1) \to K^n$ est un isomorphisme. Dans la base $\{1, X, \ldots, X^{n-1}\}$ à la source et la base canonique au but, sa matrice est la matrice de Vandermonde :*

$$V_\omega = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \omega & \ldots & \omega^{n-1} \\ \vdots & & & \vdots \\ 1 & \omega^{n-1} & \ldots & \omega^{(n-1)^2} \end{pmatrix}.$$

La matrice de l'isomorphisme inverse est $\frac{1}{n}V_{\omega^{-1}}$.

Preuve : L'image de X^i par DFT_ω est le uplet $(1, \omega^i, \ldots, \omega^{i(n-1)})$ qui est bien la i-ème colonne de la matrice de Vandermonde. Il nous reste à montrer que $V_\omega V_{\omega^{-1}} = n\mathrm{I}_n$. Pour $0 \leqslant i, j \leqslant n-1$ on calcule le coefficient (i, j) du produit $A := V_\omega V_{\omega^{-1}}$:

$$a_{i,j} = \sum_{k=0}^{n-1} \omega^{ik}\omega^{-kj} = \sum_{k=0}^{n-1} \omega^{(i-j)k}.$$

Lorsque $i \neq j$, on a $\omega^{i-j} \neq 1$ donc $a_{i,j} = \frac{\omega^{(i-j)n}-1}{\omega^{i-j}-1} = 0$. Lorsque $i = j$, $a_{i,j} = a_{i,i}$ est une somme de n termes égaux à 1, donc égal à n. Ceci termine le calcul. □

Revenons au problème du calcul du produit de deux polynômes $P, Q \in K[X]$ tels que $\deg(P) + \deg(Q) < n$, par exemple avec les degrés tous deux $< n/2$. Alors les polynômes P, Q et PQ sont tous trois égaux à leur reste dans la division euclidienne par $X^n - 1$, i.e. on peut les identifier à leur image dans $K[X]/(X^n - 1)$. Pour les multiplier, on appliquera la transformation de Fourier DFT_ω dont le calcul par l'algorithme FFT se fait en $O(n \log n)$ opérations, puis on calcule les produits des valeurs $P(\omega^i)Q(\omega^i)$ ce qui coûte n opérations, puis on interpole pour revenir en représentation dense, ce qui se fait par un algorithme FFT associé à $\mathsf{DFT}_{\omega^{-1}}$ pour un coût en $O(n \log n)$. Au total la multiplication peut être effectuée en $O(n \log n)$ opérations.

3 Vous avez dit transformation de Fourier ? !

Mais pourquoi ça s'appelle une transformée de Fourier ? Nous allons voir.

3.1 Transformation de Fourier sur $\mathbb{R}$. Soit f une fonction intégrable sur $\mathbb{R}$, à valeurs complexes. Sa transformée de Fourier est la fonction $\widehat{f}$ définie par :

$$\widehat{f}(\chi) = \frac{1}{\sqrt{2\pi}} \int_{\mathbb{R}} \mathrm{e}^{-i\chi x} f(x) \mathrm{d}x.$$

L'opération $\mathscr{F} : f \mapsto \widehat{f}$ envoie la convolution sur le produit point par point :

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

où $h = f_1 * f_2$ est définie par $h(x) = \int_{\mathbb{R}} f_1(x-t) f_2(t) \mathrm{d}t$. Soulignons que ce produit de convolution doit son existence à, ou est un reflet de, la loi de groupe de $\mathbb{R}$.

3.2 Remarques. Il y a quelques petits problèmes :

(1) Si on veut que le produit de convolution possède un élément neutre, le bon cadre est celui des distributions et le neutre est la masse de Dirac δ_0. De plus, pour $a, b \in \mathbb{R}$ on a la formule $\delta_a * \delta_b = \delta_{a+b}$ pour la convolution de deux masses de Dirac. Ceci montre bien l'interaction avec la loi de groupe.

(2) Si $f_1 \in L^1$ et $f_2 \in L^1$, alors $f_1 * f_2 \in L^1$. Mais un tel résultat de stabilité n'a pas lieu dans L^p pour $p \neq 1$. (En général, l'*inégalité de Young* dit que si $1 \leqslant p, q, r \leqslant \infty$ et $\frac{1}{p} + \frac{1}{q} = 1 + \frac{1}{r}$, alors $f \in L^p$, $g \in L^q \Longrightarrow f * g \in L^r$ et même $\|f * g\|_r \leqslant \|f\|_p \cdot \|g\|_q$. Ainsi L^p n'est stable par convolution que pour $p = 1$.) Or, on est aussi intéressé par la transformée de Fourier dans d'autres espaces, comme L^2.

Dans le cas où G est un groupe fini, tous ces problèmes disparaîtront.

3.3 Transformation de Fourier sur des groupes localement compacts. Le domaine d'intégration $G = \mathbb{R}$ est un groupe abélien, muni d'une topologie pour laquelle il est localement compact (ce qui signifie qu'il est séparé et que chaque point de G possède un voisinage compact – dans notre exemple, simplement une petite boule fermée). D'autres exemples de tels groupes sont $G = S^1 = \mathbb{U}$ le cercle unité ou groupe des complexes de module 1, ou $G = \mathbb{Z}$, ou $G = \mathbb{Z}/n\mathbb{Z}$. (Les produits finis de tels groupes sont d'autres possibilités, par exemple tous les groupes abéliens de type fini.) Or, il existe une théorie de la transformation de Fourier sur de tels groupes. Parmi les ingrédients nécessaires pour l'expliquer, figurent deux notions importantes :

3.4 Définitions. (1) Un *caractère* de G est un morphisme de groupes $\chi : G \to \mathbb{U}$.

(2) Une *mesure de Haar* sur G est une mesure borélienne positive invariante sur G, i.e. une mesure $\mu : \mathcal{B}(G) \to \mathbb{R}_{\geqslant 0}$ définie sur la tribu des boréliens de G (tribu engendrée par les ouverts), et qui est invariante i.e. $\mu(g + A) = \mu(A)$ pour tous $A \in \mathcal{B}(G)$ et $g \in G$. (Sur des groupes non abéliens, on peut distinguer invariance à droite et invariance à gauche.)

3.5 Théorème (Alfréd Haar, 1933). *Tout groupe abélien topologique localement compact G possède une mesure de Haar μ et celle-ci est unique à multiplication par un scalaire > 0 près.*

Lorsque G est compact, on a $\mu(G) < +\infty$ et on peut normaliser de sorte que $\mu(G) = 1$, ce qui la rend véritablement unique. La mesure de Haar de $G = \mathbb{R}$ est la mesure de Lebesgue λ, et la mesure de Haar de $\mathbb{U}$ est $\frac{1}{2\pi}\lambda$. Pour $G = \mathbb{Z}/n\mathbb{Z}$, la mesure de Haar est la mesure de comptage :

$$\mu(A) = \tfrac{|A|}{|G|} \quad \text{pour toute partie } A \subset G$$

$$\textstyle\int_G f \mathrm{d}\mu = \frac{1}{|G|}\sum_{g\in G} f(g) \quad \text{pour toute fonction } f : G \to \mathbb{C}.$$

Notons $\widehat{G} = \mathrm{Hom}(G, \mathbb{U})$ l'ensemble des caractères de G. Muni du produit point par point, c'est un groupe et muni de la norme de la convergence uniforme sur tout compact, il est localement compact. On définit la transformée de Fourier d'une fonction $f : G \to \mathbb{C}$ comme étant la fonction $\widehat{f} : \widehat{G} \to \mathbb{C}$ définie, pour tout caractère $\chi : G \to \mathbb{U}$, par :

$$\widehat{f}(\chi) = \int_G \chi(g) f(g) \mathrm{d}\mu.$$

Notons $F(G)$ l'ensemble des fonctions à valeurs complexes sur G qui sont intégrables (avec les nuances imposées par 3.2(2)). Ainsi, la transformée de Fourier met en correspondance deux algèbres :

$$(F(G), *) \underset{\mathscr{F}^{-1}}{\overset{\mathscr{F}}{\rightleftarrows}} (F(\widehat{G}), \cdot)\ .$$

3.6 Transformation de Fourier sur $\mathbb{U}$. Rappelons que l'exponentielle $\mathbb{R} \to \mathbb{U}$, $x \mapsto \mathrm{e}^{2i\pi x}$ est un morphisme de groupes de noyau $\mathbb{Z}$ qui identifie $\mathbb{U}$ au quotient $\mathbb{R}/\mathbb{Z}$. De même, pour tout $n \in \mathbb{Z}$, l'application $\mathbb{R} \to \mathbb{U}$, $x \mapsto \mathrm{e}^{2i\pi nx}$ est un morphisme de groupes de noyau $\mathbb{Z}$ qui induit un caractère $\chi_n : \mathbb{U} \simeq \mathbb{R}/\mathbb{Z} \to \mathbb{U}$. On montre que l'application $\mathbb{Z} \to \widehat{\mathbb{U}}$, $n \mapsto \chi_n$ est un isomorphisme de groupes (ici discrets). La transformée de Fourier d'une fonction $f : \mathbb{U} \to \mathbb{C}$ est la fonction $\widehat{f} : \widehat{\mathbb{U}} \simeq \mathbb{Z} \to \mathbb{C}$ qui associe à n son n-ème coefficient de Fourier c_n. La formule d'inversion de Fourier dit que

$$f(x) = \sum_{n\in\mathbb{Z}} c_n \mathrm{e}^{2i\pi nx}.$$

La théorie de Fourier sur $\mathbb{U}$ est simplement la théorie des séries de Fourier des fonctions périodiques.

3.7 Transformation de Fourier sur $\mathbb{Z}/n\mathbb{Z}$. Explicitons tout ceci pour $G = \mathbb{Z}/n\mathbb{Z}$. L'espace $F(G)$ est de dimension finie et la formule $f = \sum_{g\in G} f(g)\delta_g$ montre que les indicatrices δ_g, $g \in G$, forment une base. La propriété $\delta_a * \delta_b = \delta_{a+b}$ (cf 3.2(1)) permet de voir qu'on a un isomorphisme de $\mathbb{C}$-algèbres :

$$(F(\mathbb{Z}/n\mathbb{Z}), *) \xrightarrow{\sim} \frac{\mathbb{C}[X]}{(X^n - 1)}.$$

On a un isomorphisme $\widehat{G} \xrightarrow{\sim} \mu_n$, $\chi \mapsto \chi(1)$ entre le groupe dual et le groupe $\mu_n := \mu_n(\mathbb{C})$ des racines n-èmes complexes de l'unité. (L'isomorphisme inverse associe à une racine de l'unité ω le caractère défini par $\chi(i) = \omega^i$.) Il y a un isomorphisme de $\mathbb{C}$-algèbres :

$$(F(\mu_n), \cdot) = \mathbb{C}^{\mu_n} \xrightarrow{\sim} \mathbb{C}^n$$

où le but est l'algèbre produit, dans laquelle le produit se fait composante par composante. La transformée de Fourier est donc un isomorphisme

$$\frac{\mathbb{C}[X]}{(X^n - 1)} \xrightarrow{\sim} \mathbb{C}^n$$

qui n'est autre que l'isomorphisme donné par l'évaluation des polynômes en les n racines de l'unité i.e. $F \mapsto (F(1), F(\omega), \ldots, F(\omega^{n-1}))$. Ce qui explique ce que nous voulions expliquer.