

La Transformée de Fourier Rapide (FFT)

1 La transformée

La *transformée de Fourier* est une application qui transforme une fonction complexe en une autre. Plus précisément, soit $f : \mathbb{C} \rightarrow \mathbb{C}$ une applications. La transformée de Fourier classique tranforme f en $g : \mathbb{C} \rightarrow \mathbb{C}$ et est définie par

$$g(y) = \int_{-\infty}^{\infty} f(x)e^{2\pi ixy} dx$$

avec $i = \sqrt{-1}$. La tranformée de Fourier sert en systèmes linéaires, en optique, en probabilité, en physique quantique, en équations différentielles, en traitement du signal etc. Elle a un analogue discret, aussi utile dans ces même domaines.

Soit $\mathbf{a} = [a_0, \dots, a_{n-1}]$ et $\mathbf{b} = [b_0, \dots, b_{n-1}]$ deux vecteurs dans \mathbb{C}^n . Le vecteur \mathbf{b} est la tranformée de Fourier de \mathbf{a} , écrit $\mathbf{b} = F[\mathbf{a}]$, si pour $t = 0, \dots, n-1$ et $\omega = e^{\frac{2\pi i}{n}}$,

$$b_t = \sum_{s=0}^{n-1} a_s e^{\frac{2\pi i}{n}st} = \sum_{s=0}^{n-1} a_s \omega^{st}$$

où $\omega = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$ est la n -ième racine principale de l'unité.

Le vecteur \mathbf{a} peut-être interprété comme le vecteur des coefficients du polynôme $a(x) = a_0x^0 + \dots + a_{n-1}x^{n-1} = \sum_{s=0}^{n-1} a_s x^s$; le vecteur \mathbf{b} a une interprétation semblable. Les coefficients b_t sont alors des valeurs de $a(x)$ en $x = e^{\frac{2\pi i}{n}t}$. Il en résulte que les coefficients b_t peuvent être calculés avec $n-1$ multiplications et $n-1$ additions par la méthode de Horner (i.e. $p(x) = p_0x^0 + \dots + p_{n-1}x^{n-1} = \sum_{s=0}^{n-1} p_s x^s = p_0 + x(p_1 + x(p_2 + \dots + x(p_{n-2} + xp_{n-1}))$). Donc \mathbf{b} peut être calculé à partir de \mathbf{a} en $O(n^2)$ multiplications et $O(n^2)$ additions. L'algorithme connu comme *FFT*, *Fast Fourier Transform* permet de réduire ces nombres à $O(n \lg n)$.

L'algorithme repose sur le théoreme suivant, permettant le calcul de la transformée d'un vecteur de longueur n à partir des tranformées de deux vecteurs de longueur $\frac{n}{2}$.

Théorème 1.1 *Soit n pair,*

$$[b_0, b_1, \dots, b_{n-1}] = F[a_0, a_1, \dots, a_{n-1}]$$

$$[c_0, c_1, \dots, c_{\frac{n}{2}-1}] = F[a_0, a_2, \dots, a_{n-2}]$$

$$[d_0, d_1, \dots, d_{\frac{n}{2}-1}] = F[a_1, a_3, \dots, a_{n-1}]$$

et soit $\omega = e^{\frac{2\pi i}{n}}$. Alors on a

$$b_t = c_t + \omega^t d_t \quad \text{et} \quad b_{t+\frac{n}{2}} = c_t - \omega^t d_t$$

pour $t = 0, 1, \dots, \frac{n}{2} - 1$.

Démonstration: On a

$$c_t = \sum_{k=0}^{\frac{n}{2}-1} a_{2k} e^{\frac{2\pi i}{2} kt} = \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2kt} \quad \text{et} \quad d_t = \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} e^{\frac{2\pi i}{2} kt} = \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{2kt}$$

pour $t = 0, 1, \dots, \frac{n}{2} - 1$.

Donc

$$c_t + \omega^t d_t = \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2kt} + \omega^t \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{2kt} = \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2kt} + \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{(2k+1)t} = \sum_{s=0}^{n-1} a_s \omega^{st} = b_t$$

et

$$\begin{aligned} c_t - \omega^t d_t &= \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2kt} - \omega^t \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{2kt} = \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2kt} - \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{(2k+1)t} = \\ &\quad \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2kt} \omega^{kn} + \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{(2k+1)t} \omega^{(2k+1)\frac{n}{2}} = \\ &\quad \sum_{k=0}^{\frac{n}{2}-1} a_{2k} \omega^{2k(t+\frac{n}{2})} + \sum_{k=0}^{\frac{n}{2}-1} a_{2k+1} \omega^{(2k+1)(t+\frac{n}{2})} = \sum_{s=0}^{n-1} a_s \omega^{s(t+\frac{n}{2})} = b_{t+\frac{n}{2}} \end{aligned}$$

parce que $\omega^n = 1$ et $\omega^{\frac{n}{2}} = -1$. □

Le théorème suggère un algorithme pour le cas de $n = 2^p$. Si on représente les divisions par une arborescence binaire, on obtient, par exemple pour $n = 8$,

$$F[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7]$$

$$F[a_0, a_2, a_4, a_6]$$

$$F[a_1, a_3, a_5, a_7]$$

$$F[a_0, a_4]$$

$$F[a_2, a_6]$$

$$F[a_1, a_5]$$

$$F[a_3, a_7]$$

$$F[a_0]$$

$$F[a_4]$$

$$F[a_2]$$

$$F[a_6]$$

$$F[a_1]$$

$$F[a_5]$$

$$F[a_3]$$

$$F[a_7]$$

En observant que $F[c] = c$ pour toute constante $c \in \mathbb{C}$, un algorithme itératif n'est pas très difficile à obtenir: il suffit de suivre l'arborescence à l'envers, par niveau. L'observation suivante permet une implantation plus efficace de l'algorithme. Soit \mathbf{a} un vecteur dans \mathbb{C}^n . Non seulement peut-il être interprété comme un polynôme $a(x) = a_0x^0 + \dots + a_{n-1}x^{n-1} = \sum_{s=0}^{n-1} a_sx^s$, il peut également être lu comme deux polynômes de degré $\frac{n}{2}$ ($\sum_{s=0}^{\frac{n}{2}-1} a_sx^s$ et $\sum_{s=\frac{n}{2}}^{n-1} a_sx^s$), ou bien quatre polynômes de degré $\frac{n}{4}$ ($\sum_{s=0}^{\frac{n}{4}-1} a_sx^s$, $\sum_{s=\frac{n}{4}}^{\frac{n}{2}-1} a_sx^s$, $\sum_{s=\frac{n}{2}}^{\frac{3n}{4}-1} a_sx^s$, $\sum_{s=\frac{3n}{4}}^{n-1} a_sx^s$) ou huit polynômes de degré $\frac{n}{8}$ ($\sum_{s=0}^{\frac{n}{8}-1} a_sx^s$, $\sum_{s=\frac{n}{8}}^{\frac{2n}{8}-1} a_sx^s$, $\sum_{s=\frac{3n}{8}}^{\frac{4n}{8}-1} a_sx^s$, $\sum_{s=\frac{4n}{8}}^{\frac{5n}{8}-1} a_sx^s$, $\sum_{s=\frac{5n}{8}}^{\frac{6n}{8}-1} a_sx^s$, $\sum_{s=\frac{6n}{8}}^{\frac{7n}{8}-1} a_sx^s$, $\sum_{s=\frac{7n}{8}}^{n-1} a_sx^s$) etc. Nous pouvons alors utiliser un même tableau de longueur n pour représenter les vecteurs de longueurs 1 du départ, les vecteurs intermédiaires et la solution finale.

L'exemple (abstrait) de $n = 8$ mène aux changements suivants.

a_0	a_4	a_2	a_6	a_1	a_5	a_3	a_7
$F[a_0, a_4]$		$F[a_2, a_6]$		$F[a_1, a_5]$		$F[a_3, a_7]$	
$F[a_0, a_2, a_4, a_6]$				$F[a_1, a_3, a_5, a_7]$			
$F[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7]$							

Pour un exemple concret, toujours avec $n = 8$, regardons $\mathbf{a} = [2, 3, 5, 4, 1, 3, 6, 4]$. On aura les changements indiqués par les tableaux ci-dessous.

2	1	5	6	3	3	4	4
$F[2, 1]$		$F[5, 6]$		$F[3, 3]$		$F[4, 4]$	
$F[2, 5, 1, 6]$				$F[3, 4, 3, 4]$			
$F[2, 3, 5, 4, 1, 3, 6, 4]$							

2	1	5	6	3	3	4	4
3	1	11	-1	6	0	8	0
14	$1 - i$	-8	$1 + i$	14	0	-2	0
28	$1 - i$	$-8 - 2i$	$1 + i$	0	$1 - i$	$-8 + 2i$	$1 + i$

Le dernier tableau a été obtenu en appliquant le théorème trois fois, à partir de la première ligne. La deuxième ligne provient de la première, via le théorème, avec $n = 2$ et donc avec $\omega = e^{\frac{2\pi i}{2}} = \cos \frac{2\pi}{2} + i \sin \frac{2\pi}{2} = -1$, $t = 0$ (la seule valeur admise) et $\omega^t = \omega^0 = 1$. La troisième provient de la deuxième, avec $n = 4$, $\omega = e^{\frac{2\pi i}{4}} = \cos \frac{2\pi}{4} + i \sin \frac{2\pi}{4} = i$, $t = 0, 1$, $\omega^0 = 1$, $\omega^1 = i$. Pour passer de la troisième ligne à la dernière on met $n = 8$, $\omega = e^{\frac{2\pi i}{8}} = \cos \frac{2\pi}{8} + i \sin \frac{2\pi}{8} = \frac{1+i}{\sqrt{2}}$, $t = 0, 1, 2, 3$ et $\omega^0 = 1$, $\omega^1 = \frac{1+i}{\sqrt{2}}$, $\omega^2 = i$, $\omega^3 = \frac{i-1}{\sqrt{2}}$.

Pour comprendre comment le théorème s'applique, il est pratique de séparer les lignes et d'indiquer les calculs. Avec l'exemple concret on obtient le dessin de la page suivante. La i -ème ligne représente le contenu du tableau $T[0..n-1]$ après la i -ème itération. Si on "lit" le dessin du bas vers le haut, on voit les applications du théorème (on divise-pour-régner); quand on "lit" le

dessin du haut vers le bas, on voit le fonctionnement de l'algorithme itératif. Une chose à noter est l'ordre des entrées sur la première ligne: afin d'avoir $F[2, 3, 5, 4, 1, 3, 6, 4]$ à la fin, nous commençons par $[2][1][5][6][3][3][4][4]$. Essayez de découvrir la clé de cet ordre (et de prouver que c'est la bonne)! La page suivante donne un exemple abstrait pour $n = 16$

2	1	5	6	3	3	4	4
---	---	---	---	---	---	---	---

3	1	11	-1	6	0	8	0
---	---	----	----	---	---	---	---

14	$1 - i$	-8	$1 + i$	14	0	-2	0
----	---------	----	---------	----	---	----	---

28	$1 - i$	$-8 - 2i$	$1 + i$	0	$1 - i$	$-8 + 2i$	$1 + i$
----	---------	-----------	---------	---	---------	-----------	---------

a_0 a_8 a_4 a_{12} a_2 a_{10} a_6 a_{14} a_1 a_9 a_5 a_{13} a_3 a_{11} a_7 a_{15}

$F[a_0, a_8]$ $F[a_4, a_{12}]$ $F[a_2, a_{10}]$ $F[a_6, a_{14}]$ $F[a_1, a_9]$ $F[a_5, a_{13}]$ $F[a_3, a_{11}]$ $F[a_7, a_{15}]$

$F[a_0, a_4, a_8, a_{12}]$

$F[a_2, a_6, a_{10}, a_{14}]$

$F[a_1, a_5, a_9, a_{13}]$

$F[a_3, a_7, a_{11}, a_{15}]$

$F[a_0, a_2, a_4, a_6, a_8, a_{10}, a_{12}, a_{14}]$

$F[a_1, a_3, a_5, a_7, a_9, a_{11}, a_{13}, a_{15}]$

$F[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}]$

On voit assez clairement maintenant comment il faut procéder. Si $n = 2^p$ et $\mathbf{a} \in \mathbb{C}^n$, on commence par un tableau $T[0..n-1]$ rempli par $T[i] = a_{\rho(i)}$ où $\rho(i) = i_{p-1}i_{p-2}\dots i_0$ pour $i = i_0\dots i_{p-1}$, $i_j \in \{0, 1\}$ (c'est-à-dire, $\rho(i)$ est l'écriture binaire *renversée* de i sur p bits). Après, on suit le dessin en utilisant deux variables X et Y pour les calculs intermédiaires: on remplace les entrées de T par de nouvelles valeurs. Les valeurs de ω^t sont calculées au début et stockées dans un tableau $\Omega[0..n-1]$.

Première itération; le calcul des vecteurs de longueur 2^1

- $\omega = e^{\frac{2\pi i}{2^1}} = \cos \frac{2\pi}{2^1} + i \sin \frac{2\pi}{2^1} = -1$
- $\Omega[0] \leftarrow \omega^0 = 1$
-

$$X \leftarrow T[0], Y \leftarrow \Omega[0]T[1], T[0] \leftarrow X + Y, T[1] \leftarrow X - Y$$

$$X \leftarrow T[2], Y \leftarrow \Omega[0]T[3], T[2] \leftarrow X + Y, T[3] \leftarrow X - Y$$

⋮

$$X \leftarrow T[n-2], Y \leftarrow \Omega[0]T[n-1], T[n-2] \leftarrow X + Y, T[n-1] \leftarrow X - Y$$

Deuxième itération, le calcul des vecteurs de longueur 2^2

- $\omega = e^{\frac{2\pi i}{2^2}} = \cos \frac{2\pi}{2^2} + i \sin \frac{2\pi}{2^2} = i$
- $\Omega[0] \leftarrow \omega^0 = 1; \Omega[1] \leftarrow \omega^1 = i$
-

$$X \leftarrow T[0], Y \leftarrow \Omega[0]T[2], T[0] \leftarrow X + Y, T[2] \leftarrow X - Y$$

$$X \leftarrow T[1], Y \leftarrow \Omega[0]T[3], T[1] \leftarrow X + Y, T[3] \leftarrow X - Y$$

$$X \leftarrow T[4], Y \leftarrow \Omega[1]T[6], T[4] \leftarrow X + Y, T[6] \leftarrow X - Y$$

$$X \leftarrow T[5], Y \leftarrow \Omega[1]T[7], T[5] \leftarrow X + Y, T[7] \leftarrow X - Y$$

⋮

$$X \leftarrow T[n-4], Y \leftarrow \Omega[0]T[n-2], T[n-4] \leftarrow X + Y, T[n-2] \leftarrow X - Y$$

$$X \leftarrow T[n-3], Y \leftarrow \Omega[1]T[n-1], T[n-3] \leftarrow X + Y, T[n-1] \leftarrow X - Y$$

⋮

k -ème itération, le calcul des vecteurs de longueur 2^k

- $\omega = e^{\frac{2\pi i}{2^k}} = \cos \frac{2\pi}{2^k} + i \sin \frac{2\pi}{2^k}$

- $\Omega[j] \leftarrow \omega^j = 1, j = 0, \dots, 2^{k-1} - 1$
-

$$\begin{aligned}
& X \leftarrow T[0], Y \leftarrow \Omega[0]T[2^{k-1}], T[0] \leftarrow X + Y, T[2^k] \leftarrow X - Y \\
& X \leftarrow T[1], Y \leftarrow \Omega[1]T[2^{k-1} + 1], T[1] \leftarrow X + Y, T[2^{k-1} + 1] \leftarrow X - Y \\
& X \leftarrow T[2], Y \leftarrow \Omega[1]T[2^{k-1} + 2], T[2] \leftarrow X + Y, T[2^{k-1} + 2] \leftarrow X - Y \\
& X \leftarrow T[3], Y \leftarrow \Omega[1]T[2^{k-1} + 3], T[3] \leftarrow X + Y, T[2^{k-1} + 3] \leftarrow X - Y \\
& \quad \vdots \\
& X \leftarrow T[n - 2^k], Y \leftarrow \Omega[2^{k-1} - 1]T[n - 2^{k-1}], T[n - 2^k] \leftarrow X + Y, T[n - 2^{k-1}] \leftarrow X - Y \\
& \quad \vdots \\
& X \leftarrow T[n - 2^{k-1} - 1], Y \leftarrow \Omega[2^{k-1}]T[n - 1], T[n - 2^{k-1} - 1] \leftarrow X + Y, T[n - 1] \leftarrow X - Y
\end{aligned}$$

Pour revenir à notre exemple, on fait les calculs suivants.

1. $k = 1$: $\omega \leftarrow e^{\frac{2\pi i}{1}} = \cos \frac{2\pi}{1} + i \sin \frac{2\pi}{1} = -1$; $\Omega[0] \leftarrow 1$ et

- $F[a_0, a_4]$ est calculée par

$$X \leftarrow T[0] = 2, Y \leftarrow \Omega[0]T[1] = 1, T[0] \leftarrow X + Y = 3, T[1] \leftarrow X - Y = 1$$

- $F[a_2, a_6]$ est calculée par

$$X \leftarrow T[2] = 5, Y \leftarrow \Omega[0]T[3] = 6, T[2] \leftarrow X + Y = 11, T[3] \leftarrow X - Y = -1$$

- $F[a_1, a_5]$ est calculée par

$$X \leftarrow T[4] = 3, Y \leftarrow \Omega[0]T[5] = 3, T[4] \leftarrow X + Y = 6, T[5] \leftarrow X - Y = 0$$

- $F[a_3, a_7]$ est calculée par

$$X \leftarrow T[6] = 4, Y \leftarrow \Omega[0]T[7] = 4, T[6] \leftarrow X + Y = 8, T[7] \leftarrow X - Y = 0$$

2. $k = 2$: $\omega \leftarrow e^{\frac{2\pi i}{2}} = \cos \frac{2\pi}{2} + i \sin \frac{2\pi}{2} = i$; $\Omega[0] \leftarrow 1, \Omega[1] \leftarrow i$ et

- $F[a_0, a_2, a_4, a_6]$ est calculée par

$$X \leftarrow T[0] = 3, Y \leftarrow \Omega[0]T[2] = 11, T[0] \leftarrow X + Y = 14, T[2] \leftarrow X - Y = -8$$

$$X \leftarrow T[1] = 1, Y \leftarrow \Omega[1]T[3] = -i, T[1] \leftarrow X + Y = 1 - i, T[3] \leftarrow X - Y = 1 + i$$

- $F[a_1, a_3, a_5, a_7]$ est calculée par

$$X \leftarrow T[4] = 6, Y \leftarrow \Omega[0]T[6] = 8, T[4] \leftarrow X + Y = 14, T[6] \leftarrow X - Y = -2$$

$$X \leftarrow T[5] = 0, Y \leftarrow \Omega[1]T[7] = 0, T[7] \leftarrow X + Y = 0, T[7] \leftarrow X - Y = 0$$

3. $k = 3$: $\omega \leftarrow e^{\frac{2\pi i}{8}} = \cos \frac{2\pi}{8} + i \sin \frac{2\pi}{8} = \frac{1+i}{\sqrt{2}}$; $\Omega[0] \leftarrow 1$, $\Omega[1] \leftarrow \frac{1+i}{\sqrt{2}}$, $\Omega[2] \leftarrow i$, $\Omega[3] \leftarrow \frac{i-1}{\sqrt{2}}$ et
4. $F[a_0, a_1, a_2, a_3, a_4, a_5, a_6, a_7]$ est calculée par

$$X \leftarrow T[0] = 14, Y \leftarrow \Omega[0]T[4] = 14, T[0] \leftarrow X + Y = 28, T[4] \leftarrow X - Y = 0$$

$$X \leftarrow T[1] = 1 - i, Y \leftarrow \Omega[1]T[5] = 0, T[1] \leftarrow X + Y = 1 - i, T[5] \leftarrow X - Y = 1 - i$$

$$X \leftarrow T[2] = -8, Y \leftarrow \Omega[2]T[6] = -2, T[2] \leftarrow X + Y = -8 - 2i, T[6] \leftarrow X - Y = -8 + 2i$$

$$X \leftarrow T[3] = 1 + i, Y \leftarrow \Omega[3]T[7] = 0, T[3] \leftarrow X + Y = 1 + i, T[7] \leftarrow X - Y = 1 + i$$

L'algorithme général peut être écrit comme ceci (étant donné le vecteur $\mathbf{a} = [a_0, \dots, a_{n-1}]$ avec $n = 2^p$).

Algorithme 1.1 1. pour $j = 0 \dots n - 1$ faire $T[j] \leftarrow a_{\rho(j)}$

2. $\Omega[0] \leftarrow 1$, $\omega \leftarrow e^{\frac{2\pi i}{n}}$

3. pour $c = 2 \dots \frac{n}{2} - 1$ faire $\Omega[c] \leftarrow \Omega[c - 1]\Omega[1]$

4. pour $k = 1 \dots p$ faire

(a) $m \leftarrow 2^k$

(b) pour $v = 0 \dots \frac{n}{m} - 1$ faire

i. pour $j = 0 \dots \frac{m}{2} - 1$ faire

A. $X \leftarrow T[vm + j]$, $Y \leftarrow \Omega[\frac{mj}{m}]T[vm + j + \frac{m}{2}]$

B. $T[vm + j] \leftarrow X + Y$, $T[vm + j + \frac{m}{2}] \leftarrow X - Y$

5. pour $j = 0, \dots, n - 1$ faire $b_j \leftarrow T[j]$

Exercice 1.1 Prouvez que la complexité de cet algorithme est dans $O(n \lg n)$

L'ordre dans lequel on met les a_j dans T au départ semble étrange. Prouvons que c'est le bon, c'est-à-dire, prouvons que a_j doit aller dans $T_{\rho_p(j)}$ où $\rho_p(j) = j_{p-1} \dots j_0$ et $j = j_0 \dots j_{p-1}$ en binaire, avec $n = 2^p$. Écrivons $2\rho_p(j)$ pour deux fois $\rho_p(j)$, i.e., $j_{p-1} \dots j_0 0$, et, dans la même logique, $2\rho_p(j) + 1$ pour $j_{p-1} \dots j_0 1$.

Théorème 1.2 Si, dans l'algorithme 1.1, $T[j] \leftarrow a_{\rho_p(j)}$ alors, après la p -ème itération, l'algorithme produit $T[j] = b_j$ tel que $[b_0, \dots, b_{2^p-1}] = F[a_0, \dots, a_{2^p-1}]$

Démonstration: Le théorème est évidemment vrai pour $p = 0$ (pourquoi?). Supposons la propriété vraie pour p et prouvons la pour $p + 1$.

Par le théorème 1.1, $F[a_0, \dots, a_{2^{p+1}-1}]$ est obtenu à la $(p + 1)$ -ème itération de l'algorithme à partir de $F[a_0, a_2, a_4, \dots, a_{2k}, \dots, a_{2^{p+1}-2}]$ et $F[a_1, a_3, a_5, \dots, a_{2k+1}, \dots, a_{2^{p+1}-1}]$, pourvu que ces dernières soient calculées correctement. Soit T_0 et T_1 les tableaux permettant les calculs de $F[a_0, a_2, a_4, \dots, a_{2k}, \dots, a_{2^{p+1}-2}]$ et de $F[a_1, a_3, a_5, \dots, a_{2k+1}, \dots, a_{2^{p+1}-1}]$. Par l'hypothèse d'induction, on a

$$T_0[j] = a_{2\rho_p(j)} \text{ et } T_1[j] = a_{2\rho_p(j)+1}.$$

(*Exercice: vérifiez ceci!*)

Soit T le tableau obtenu par la concatenation de T_0 et T_1 , i.e. soit $T[j] = T_0[j]$ pour $j = 0, \dots, 2^p - 1$ et $T[j] = T_1[j - 2^p]$ pour $j = 2^p, \dots, 2^{p+1} - 1$. On a alors

$$T[j] = a_{2^{\rho_p(j)}} = a_{\rho_{p+1}(j)} \text{ pour } j = 0, \dots, 2^p - 1$$

et

$$T[j] = a_{2^{\rho_p(j)+1}} = a_{\rho_{p+1}(j)} \text{ pour } j = 2^p, \dots, 2^{p+1} - 1$$

Il est - ou il doit être - clair qu'en commençant par T , l'algorithme va trouver $F[a_0, \dots, a_{n-1}]$. \square

2 La transformée inverse

Il est peut-être surprenant qu'essentiellement le même algorithme calcule la transformée de Fourier inverse. Tout devient clair dans le théorème suivant.

Théorème 2.1 *Soit*

$$a_s = \frac{1}{n} \sum_{t=0}^{n-1} b_t e^{-\frac{2\pi i}{n} st} = \frac{1}{n} \sum_{t=0}^{n-1} b_t \omega^{-st}$$

pour $s = 0, \dots, n - 1$. Alors

$$[b_0, b_1, \dots, b_{n-1}] = F[a_0, a_1, \dots, a_{n-1}].$$

Démonstration: Soit c_k la k -ème coordonnée de $F[a_0, a_1, \dots, a_{n-1}]$. Alors

$$c_k = \sum_{s=0}^{n-1} \left(\frac{1}{n} \sum_{t=0}^{n-1} b_t e^{-\frac{2\pi i}{n} st} \right) e^{\frac{2\pi i}{n} sk} = \sum_{t=0}^{n-1} \left(\frac{1}{n} \sum_{s=0}^{n-1} e^{\frac{2\pi i}{n} s(k-t)} \right) b_t$$

et il suffira de prouver que

$$\frac{1}{n} \sum_{s=0}^{n-1} e^{\frac{2\pi i}{n} s(k-t)} = \begin{cases} 1 & \text{pour } k = t \\ 0 & \text{pour } k \neq t \end{cases}$$

pour que le théorème soit démontré. Pour $k = t$ l'égalité est évidente; regardons alors le cas $k \neq t$. Dans ce cas $z = e^{\frac{2\pi i}{n}(k-t)} \neq 1$ et

$$(z - 1) \sum_{s=0}^{n-1} z^s = z^n - 1 = 0$$

ce qui signifie que $\sum_{s=0}^{n-1} z^s = 0$ et la preuve est terminée. \square

Pour calculer $F^{-1}[b_0, b_1, \dots, b_{n-1}] = [a_0, a_1, \dots, a_{n-1}]$ on se sert de l'algorithme FFT 1.1 avec les changements suivants:

- $T[j] \leftarrow b_{\rho(j)}$ dans l'initialisation
- $\Omega[1] \leftarrow e^{-\frac{2\pi i}{n}}$ pour calculer les ω^t

- $a_j \leftarrow \frac{1}{n}T[j]$ en sortie

Pour voir que ces changements suffisent (et sont nécessaires) on peut prouver un théorème qui ressemble au Théorème 1.1. Il est également possible de regarder les opérations inverses dans l'algorithme FFT et comprendre comment interviennent les changements indiqués, toujours avec la supposition que $n = 2^p$.

Exercice 2.1 Pourquoi la restriction $n = 2^p$ n'en est pas une?

3 Un exemple

Soit $A(x) = \sum_{i=0}^r a_i x^i$, $B(x) = \sum_{j=0}^s b_j x^j$ et $C(x) = A(x)B(x)$. Alors

$$C(x) = \sum_{k=0}^{r+s} c_k x^k \quad \text{et} \quad c_k = \sum_{i+j=k} a_i b_j, \quad \text{pour } k = 0, \dots, r+s.$$

Chaque c_k peut être calculé avec $(r+1)(s+1)$ multiplications et rs additions. Une manière plus rapide est de remplir A et B de zéros pour que les degrés deviennent des puissances de 2 et de passer par la Transformée de Fourier rapide.

Soit $n = 2^{\lceil \lg(r+s) \rceil}$ et soit

$$A(x) = \sum_{i=0}^{n-1} a_i x^i, \quad B(x) = \sum_{j=0}^{n-1} b_j x^j, \quad C(x) = \sum_{k=0}^{n-1} c_k x^k$$

avec $c_k = b_j = a_i = 0$ pour $k > r+s, j > s, i > r$. Soit

$$[a_0^*, \dots, a_{n-1}^*] = F[a_0, \dots, a_{n-1}]$$

$$[b_0^*, \dots, b_{n-1}^*] = F[b_0, \dots, b_{n-1}]$$

$$[c_0^*, \dots, c_{n-1}^*] = F[c_0, \dots, c_{n-1}]$$

et soit $z = e^{\frac{2\pi i}{n}}$. Alors, par définition,

$$a_k^* = A(z^k), \quad b_k^* = B(z^k) \quad \text{et} \quad c_k^* = C(z^k)$$

et on note que $c_k^* = a_k^* b_k^*$, parce qu'il s'agit d'une valeur d'un polynôme évalué à z^k de deux façons différentes. Donc pour calculer $A(x)B(x)$, on trouve c_0, \dots, c_{n-1} en calculant

- $[a_0^*, \dots, a_{n-1}^*] = \mathbf{a}^*$ à partir de $[a_0, \dots, a_{n-1}]$ (FFT)
- $[b_0^*, \dots, b_{n-1}^*] = \mathbf{b}^*$ à partir de $[b_0, \dots, b_{n-1}]$ (FFT)
- $[c_0^*, \dots, c_{n-1}^*] = \mathbf{c}^*$ à partir de \mathbf{a}^* et \mathbf{b}^* ($c_k^* = a_k^* b_k^*$)
- $[c_0, \dots, c_{n-1}]$ à partir de $[c_0^*, \dots, c_{n-1}^*]$ (FFT inverse)

Tout ceci prends $n + 3\frac{n}{2} \lg n$ multiplications et $3n \lg n$ additions. Puisque $n \leq 2(r+s)$, l'amélioration est considérable quand la somme $r+s$ est assez grande.

4 Les racines

Une racine n -ème principale d'unité est $\omega = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$. Elle est *principale* parce que toutes les autres racines n -ème de l'unité sont obtenues comme des puissances de ω . Voici un petit tableau pour les petites puissances de 2:

- $n = 2$ $\omega = e^{\frac{2\pi i}{2}} = -1$
- $n = 4$ $\omega = e^{\frac{2\pi i}{4}} = i$
- $n = 8$ $\omega = e^{\frac{2\pi i}{8}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$
- $n = 16$ $\omega = e^{\frac{2\pi i}{16}} = \frac{\sqrt{2+\sqrt{2}}}{2} + i\frac{\sqrt{2-\sqrt{2}}}{2}$