Une méthode rapide de multiplication des polynômes.

Rémi Lajugie

Définition 1 *On appelle représentation par valeur d'un polynôme P, la donnée de deux n-uplet $(x_1, \dots, x_n)$ et $(P(x_1), \dots, P(x_n))$. Par contraste, la donnée de la suite des coefficients, s'appelle une représentation par coefficients.*

Proposition 1 *Soit $(y_1, \dots, y_n) \in \mathbb{C}^n$. Par n points distincts $(x_1, \dots, x_n)$ il passe un unique polynôme de degré au plus $n-1$ prenant la valeur y_i en chaque x_i.*

Preuve : cela résulte du fait que les formes linéaires $P \mapsto P(x_i)$ sont une base de l'espace dual $\mathbb{R}_{n-1}[X]^*$ dont la base antéduale est la base des polynômes interpolateurs de Lagrange.

Conséquence : la représentation par valeur d'un polynôme P est univoque dès que le nombre de points est strictement supérieur au degré.

Proposition 2 *Soit deux polynômes P, Q de degré au plus $n-1$, représentés par valeurs en $2n-1$ points. Alors une représentation par valeur de PQ est donné par le $2n-1$ uplet des $(P(x_i)Q(x_i))_{i \in \{1,\dots,2n-1\}}$.*

Définition 2 *On appelle interpolation d'un polynôme de degré au plus $n-1$ représenté par valeurs en $k \geq n$ points, l'application qui associe la représentation par coefficients à la représentation par valeurs en $(x_1, \dots, x_k)$.*

Remarque : l'interpolation revient à résoudre un système linéaire de Vandermonde.

$$\begin{pmatrix} P(x_1) \\ \vdots \\ P(x_n) \end{pmatrix} = \begin{pmatrix} x_1 & \dots & x_1^n \\ \vdots & \vdots & \vdots \\ x_n & \dots & x_n^n \end{pmatrix} \begin{pmatrix} a_0 \\ \vdots \\ a_{n-1} \end{pmatrix}.$$

Théorème 1 *L'opérateur de transformée de Fourier inverse discrète réalise l'interpolation aux points $\xi, \dots, \xi_k$ où les ξ_k sont les racines $k-$ èmes complexes de l'unité.*

Preuve : La transformée de Fourier résout précisément un problème de multiplication matricielle.

Théorème 2 *Soit P, Q de degré $2^p - 1$. Il existe un algorithme coûtant $O(nlog(n))$ multiplications permettant de multiplier P et Q.*

L'algorithme est le suivant :

1. Effectuer la transformation de Fourier de P et Q d'ordre 2^{p+1}.
2. Multiplier les représentations par valeurs.
3. Interpoler par la transformation de Fourier inverse.

Preuve :

Etape 1 : correction de l'algorithme

Par les propositions précédentes, à la fin de l'opération 2, on a une représentation univoque de PQ puisque $deg(PQ) < 2^{p+1}$ et que l'on a 2^{p+1} points d'interpolation. Par le théorème, la transformée de Fourier inverse nous donne la représentation par coefficients du polynôme PQ.

Etape 2 : complexité de l'algorithme

L'opération 1 coûte $O(n\log(n))$ opérations car, vu la récursion de Cooley Tuckey, la complexité C_k de calculer une transformée de Fourier discrète de taille 2^k satisfait la relation de récurrence :

$$C_{k+1} = 2C_k + K2^k,$$

il vient alors, en posant $D_k = \frac{C_k}{2^k}$ que $C_k = K(2^k k)$ où K est une constante numérique.

Le coût de l'opération 2 est de 2^k multiplications.

Le coût de l'opération 3 est le même que celui de l'opération 1.

Références

— Cormen Riverson Stein.