Transformée de Fourier Rapide ou FFT

Laure Danthony et Clément Ménier

Table des matières

1 Le problème

1.1 Description

On se donne deux polynômes P et Q de degré n, il s'agit de calculer le produit PQ.

1.2 Méthode naïve

La méthode naïve qui consiste à appliquer la formule des expressions des coefficients est en $O(n^2)$.

1.3 Méthode sioux

La méthode de Karatsuba vue il y a quelque temps est en $O(n^{1.5})$

2 Principe de la méthode

2.1 Deux caractérisations d'un polynôme de degré n

Un polynôme de degré n peut être caractérisé par des coefficients ou par la donnée de $n+1$ points.

2.2 Le diagramme de la méthode

La ruse utilisée consiste à agrandir le chemin afin de réduire le temps pour le parcourir. L'évaluation et l'interpolation "naïves" sont effectuées en $O(n^2)$ alors que la méthode qui va suivre va les effectuer en $O(n \ln n)$

$$\begin{array}{ccc} P = \sum a_i X^i, Q = \sum b_i X^i & \xrightarrow[n^2]{c_i = \sum a_i b_{k-i}} & PQ = \sum c_i X^i \\ \text{Eval. FFT} \downarrow n \ln n & & \text{Interp. FFT} \uparrow n \ln n \\ \big(\alpha_i = P(\omega_i)\big), \big(\beta_i = Q(\omega_i)\big) & \xrightarrow[n]{\gamma_i = \alpha_i \beta_i} & \big(\gamma_i = PQ(\omega_i)\big) \end{array}$$

2.3 Idées

- On va évaluéer les polynômes P et Q sur des nombres non quelconques (les racines n-ièmes de l'unité)
- Dans toute la suite, on travaille *uniquement* sur le polynôme $P = \sum_{i=0}^{n-1} a_i X^i$. L'évaluation de Q s'effectue de manière similaire.
- On va évaluer P en $2n-1$ points avec un algorithme en $n \ln n$.

3 Résultats algébriques importants

3.1 Notion de racine n-ième primitive

DÉFINITION 1
Soit $(R, +, ., 0, 1)$ un anneau commutatif. On dit que ω est une racine n-ième primitive si :

$$\omega^n = 1, \omega \neq 1, \forall j \in [1, n], \sum_{j=0}^{n-1} \omega^{jp} = 0$$

EXEMPLE 1 *En particulier, dans $\mathbb{C}$, les $e^{i\frac{2k\pi}{n}}$, $k \wedge n = 1$ le sont.*

REMARQUE 1 Si ω est une racine n-ième primitive, les racines n-ièmes sont :

$$1, \omega, \omega^2, \dots, \omega^{n-1}$$

DÉFINITION 2
Soit $a = (a_0, a_1, \dots, a_{n-1})$, on note $F(a) = Da$ où D est la matrice $D_{i,j} = \omega^{ij}$.

LEMME 1 *On a trivialement $F(a)_i = \sum_{k=0}^{n-1} a_k \omega^{ik}$*

PROPOSITION 1 *Soit ω une racine n-ième primitive dans R. Si n^{-1} existe dans R, alors D^{-1} existe et on a le résultat :*

$$D^{-1}_{i,j} = \frac{1}{n}\omega^{-ij}$$

PREUVE :

$$\left(DD^{-1}\right)_{i,j} = \frac{1}{n}\sum_{k=0}^{n-1} \omega^{ik}\omega^{-kj}$$

Donc, si $i = j$, elle vaut 1 et si $i \neq j$, la quantité $\sum_{k=0}^{n-1} \omega^{kp}$, pour $p = i - j$, soit $-n < p < n, p \neq 0$ vaut 0 par définition de ω. ■

3.2 Convolution

DÉFINITION 3
Soit $a = (a_0, a_1, \dots, a_{n-1})$ et $b = (b_0, b_1, \dots, b_{n-1})$. On appelle convolution de a et b noté $a \otimes b$ la quantité $c = (c_0, c_1, \dots, c_{2n-1})$ telle que :

$$c_i = \sum_{j=0}^{2n-1} a_j b_{i-j}$$

avec $a_k = b_k = 0$ si $k < 0$ ou $k > n - 1$(donc $c_{2n-1} = 0$).

THÉORÈME 1 *Si $a = (a_0, a_1, \dots, a_{n-1}, 0, \dots, 0)$ et $b = (b_0, b_1, \dots, b_{n-1}, 0, \dots, 0)$ (avec $n - 1$ zéros), alors $a \oplus b = F^{-1}\big(F(a)F(b)\big)$*

PREUVE :

$$F(a) = (a'_0, \ldots, a'_{n-1})$$
$$F(b) = (b'_0, \ldots, b'_{n-1})$$
$$a \oplus b = (c_0, \ldots, c_{2n-1})$$
$$F(a \oplus b) = (c'_0, \ldots, c'_{2n-1})$$

On note $F(a \oplus b) = F(a) \times F(b)$. Alors on a:

$$a'_l = \sum_{j=0}^{n-1} a_j \omega^{lj}$$

$$b'_l = \sum_{k=0}^{n-1} b_k \omega^{lk}$$

D'où $a'_l \times b'_l = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} a_j b_k \omega^{l(j+k)}$

Or $c_l = \sum_{j=0}^{2n-1} a_j b_{l-j}$

Donc

$$\begin{aligned} c'_l &= \sum_{p=0}^{2n-1} \sum_{j=0}^{2n-1} a_j b_{p-j} \omega^{pl} \\ &= \sum_{j=0}^{2n-1} \sum_{k=-j}^{2n-1-j} a_j b_k \omega^{l(j+k)} \\ &= \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} a_j b_k \omega^{l(j+k)} \text{ (à cause des coefficients nuls)} \\ &= a'_l \times b'_l \end{aligned}$$

■

4 FFT

4.1 Idée

- Evaluer $F(a)$ revient à calculer $P(x)$ en $x = \omega^0, x = \omega^1, \ldots, x = \omega^{n-1}$, ou encore calculer le reste de la division euclidienne de $P(X)$ par$(X-\omega^0)$,$X-\omega^1)$, ... En effet, $P(X) = Q(X)(X - \omega^i) + R_i(X)$ et $P(\omega^i) = R_i(\omega^i)$.
- Ensuite on utilisera la méthode de diviser pour régner en s'arrangeant pour que les produits partiels soient du type $X^j - \omega^i$.

4.2 Méthode

Supposons $n = 2^k$, on cherche une permutation $(c_0, c_1, \ldots, c_{n-1})$ de $(\omega_0, \omega_1, \ldots, \omega_{n-1})$.

NOTATIONS. On note

- $q_{0,k} = P$
- $q_{l,0} = X - c_l$

- $q_{l,m} = \prod_{j=l}^{l+2^m-1} (X - c_j)$ avec $0 \leq m \leq k$, l multiple de 2^m tel que $0 \leq l \leq 2^k - 1 = n - 1$.
- $r_{l,m}$ le reste de la division de P par $q_{l,m}$.

REMARQUE 2 Il s'agit de calculer les $r_{l,0}$. On les calcule par méthode descendante à l'aide de la proposition suivante.

PROPOSITION 2

$$q_{l,m} = q_{l,m-1} \times q_{l+2^{m-1},l-1}$$

$r_{l,m-1}$ est le reste de la division par $q_{l,m-1}$ de $r_{l,m}$

PREUVE : Notons $q' = q_{l,m-1}$, et $q'' = q_{l+2^{m-1},m-1}$. Alors on a par définition $P = k_1 q' + r_{l,m-1}$ et $P = kq'q'' + r_{l,m}$. Or si $r_{l,m} = k_2 q' + r$ où $deg(r) < deg(q')$, alors $P = (kq'' + k_2)q' + r$ et donc $r = r_{l,m}$. ■

DÉFINITION 4
Soit $0 \leq j < 2^k$ et $[d_0, d_1, \ldots, d_{k-1}]$ sa représentation binaire : $j = \sum_{i=0}^{k-1} d_{k-1-i} 2^i$. Alors on appelle $rev(j)$ la quantité $rev(j) = [d_{k-1}, \ldots, d_0]$.

PROPOSITION 3

$$q_{l,m} = X^{2^m} - \omega^{rev(\frac{l}{2^m})}$$

PREUVE : Par récurrence sur m en utilisant les résultats suivants : (les nombres sont codés sur k bits)

- $rev\left(\frac{l}{2^{m-1}} + 1\right) = 2^{k-1} + rev\left(\frac{l}{2^{m-1}}\right)$
- $\omega^{2^{k-1}} = -1$
- si x pair, $2rev(x) = rev(\frac{x}{2})$

■

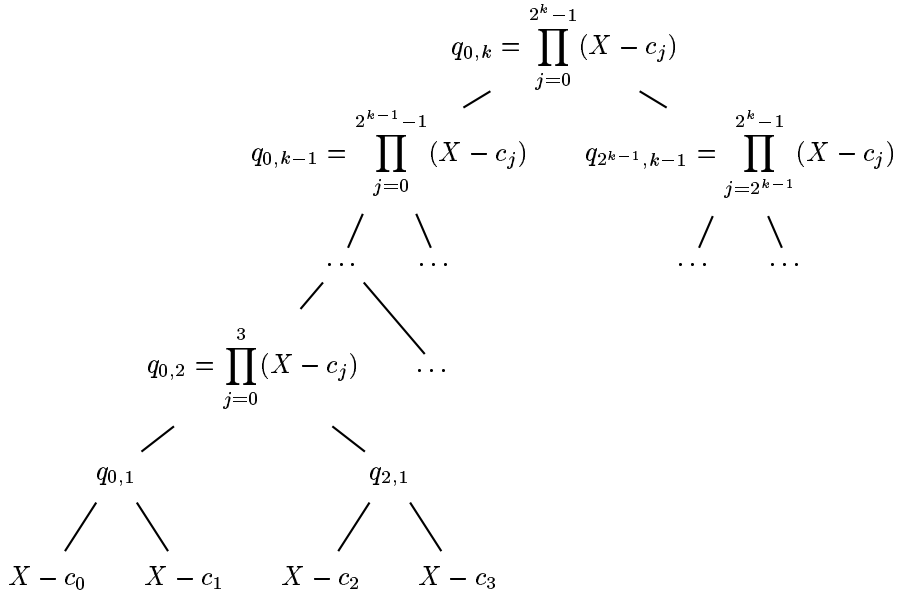
PROPOSITION 4 *Soit $P = \sum_{j=0}^{d} a_j X^j$. Alors le reste de la division de P par $X^t - c$ est :*

$$r = \sum_{j=0}^{t-1} (a_j + c a_{j+t}) X^j.$$

4.3 Résumé de la méthode

Nous désirons calculer les valeurs $P(c_i)$ en passant par le reste $r_{i,0}$ de la division de P par $X - c_i$. Pour se faire on utilise la proposition 2 pour faire le calcul des $r_{l,m}$ par dichotomie. Grâce à la permutation dûe à rev, le calcul des restes de $r_{l,m}$ par $q_{l,m-1}$ sont faciles (proposition 3 et 4).

Voici l'arbre de calcul :



4.4 Algorithme sur les polynômes

Voici l'algorithme (enfin !) :

$r_{0,k} \leftarrow \sum_{j=0}^{2^n-1} a_j X^j$
for $m = k-1$ downto 0 do
  for $l = 0$ to $n-1$ step 2^{m+1} do
    $\sum_{j=0}^{2^{m+1}-1} a_j X^j \leftarrow l, m+1$
    $s \leftarrow rev(\frac{l}{2^m})$
    $r_{l,m} \leftarrow \sum_{j=0}^{2^m-1}(a_j + \omega^s a_{j+2^m})X^j$
  for $l = 0$ to $n-1$ do
    $b_{rev(l)} \leftarrow r_{l,0}$

PROPOSITION 5 *Cet algorithme est en* $n \log n$.

REMARQUE 3 On peut aussi tabuler une liste des coefficients des polynômes vu que l'on ne se sert pas de l'indéterminée.