Développement : Transformée de Fourier rapide

Pierron Théo – Huguet Lauriane

10 décembre 2013

1 Représentations des polynômes

La donnée d'un polynôme de degré n est équivalente à la donnée de $n+1$ couples (point, valeur).

Sous la forme d'un tableau de coefficients, l'addition se fait en $O(n)$ et la multiplication en $O(n^2)$.

Sous la forme de couples, l'addition et la multiplication se font en $O(n)$:

$(x_k, P(x_k)) + (x_k, Q(x_k)) = (x_k, P(x_k) + Q(x_k))$ et $(x_k, P(x_k)) \times (x_k, Q(x_k)) = (x_k, P(x_k)Q(x_k))$.

On va utiliser la transformée de Fourier pour passer d'une représentation à l'autre :

$$\begin{tikzcd}
P = (p_k)_k, Q = (q_k)_k \arrow[r, "\text{évaluation}"] \arrow[d, "\times \text{ en } O(n^2)"] & (P(x_k))_k, (Q(x_k))_k \arrow[d, "\times \text{ en } O(n)"] \\
PQ = \left(\displaystyle\sum_{i+j=k} p_i q_j\right)_k & (PQ(x_k))_k \arrow[l, "\text{interpolation}"']
\end{tikzcd}$$

2 Évaluation

On suppose par la suite que $n+1$ est une puissance de 2. On décompose $P = P_0(X^2) + XP_1(X^2)$.

Si on a évalué P en x, on peut facilement évaluer P en $-x$ via :

$$P(x) = P_0(x^2) + xP_1(x^2) \text{ et } P(-x) = P_0(x^2) - xP_1(x^2).$$

Si on veut évaluer P en $x_0, \dots, x_n$, si on suppose $x_{i+\frac{n+1}{2}} = -x_i$, il suffit de calculer P_0 et P_1 en $x_0^2, \dots, x_{\frac{n-1}{2}}^2$, puis de sommer.

On a donc $T(n) = 2T(\frac{n+1}{2}) + O(n)$. Attention, cette relation n'est valable que pour ce n. On ne peut conclure directement, sauf si on choisit les x tels que

$$\forall i \leqslant \frac{n+1}{2^k}, x_i^{2^{k-1}} = -x_{\frac{n+1}{2^k}+i}^{2^{k-1}}. \tag{1}$$

Soit ω une racine $(n+1)$-ème de l'unité et $x_i = \omega^i$. Alors $x_{i+\frac{n+1}{2}} = -x_i$ et pour tout i, x_i^2 est une racine $\frac{n+1}{2}$-ème de l'unité donc on a la formule 1. Ainsi, la relation

$$T(n) = 2T\left(\frac{n+1}{2}\right) + O(n)$$

est vraie pour tout n (tel que $n+1$ est une puissance de 2). Alors $T(n) = O(n\log(n))$. On en déduit l'algorithme :

Algorithme 1: Eval(P, ω_0)

Entrées : Un polynôme P de degré n tel que $n+1$ est une puissance de 2 et ω_0 une racine $(n+1)$-ème primitive de l'unité

Sorties : Les $P(\omega_0^k)$

si $\deg P = 0$ **alors**
  retourner P
sinon
  Décomposer $P = P_0(X^2) + XP_1(X^2)$
  $y^0 \leftarrow \text{Eval}(P_0)$
  $y^1 \leftarrow \text{Eval}(P_1)$
  $\omega \leftarrow 1$
  pour $k = 0 \cdots \frac{n-1}{2}$ **faire**
    $y_k \leftarrow y_k^0 + \omega y_k^1$
    $y_{k+\frac{n}{2}} \leftarrow y_k^0 - \omega y_k^1$
    $\omega \leftarrow \omega\omega_0$
  retourner y

3 Interpolation

y est l'image du vecteur colonne des coefficients de P par la matrice $M_n(\omega) = (\omega^{(i-1)(j-1)})_{i,j \leqslant n+1}$.

M est une matrice de Vandermonde donc $\det(M) = \prod\limits_{i<j}(\omega^i - \omega^j) \neq 0$. M est donc inversible.

Lemme 1
On a $M_n(\omega)^{-1} = \frac{1}{n+1} M_n(\omega^{-1})$.

Démonstration. Le coefficient d'indice (i,j) dans le produit $M_n(\omega)M_n(\omega^{-1})$ est

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

Si $i = j$, cette somme vaut $n+1$. Sinon, c'est une somme géométrique qui vaut

$$\frac{\omega^{(i-j)(n+1)} - 1}{\omega^{i-j} - 1} = 0.$$ ■

Ainsi, interpoler revient à évaluer en d'autres points.

4 L'algorithme

Algorithme 2: Mult(P, Q)

Compléter P et Q avec des coefficients nuls pour avoir $n := \deg P = \deg Q$ et $n+1$ une puissance de 2.
On évalue P et Q en $(\omega^k)_k$ où ω est une racine $2(n+1)$-ème primitive de l'unité.
Enfin, on évalue $(\frac{P(\omega^k)Q(\omega^k)}{n+1})_k$ en les $(\omega^{-k})_k$.

Cet algorithme est donc en $O(n\log(n)) + O(n) + O(n\log(n)) = O(n\log(n))$.