TD 5 : Transformée de Fourier rapide

1 Calcul des n premières dérivées en un point

Exercice 1 Étant donnés la représentation par coefficients $(a_0, a_1, \ldots, a_{n-1})$ d'un polynôme A et un point x_0, on souhaite déterminer $A^{(k)}(x_0)$, la dérivée $t$ième de A en x_0, pour tous les $k \in \{0, 1, \ldots, n-1\}$.

1. Connaissant des coefficients $b_0, b_1, \ldots, b_{n-1}$ tels que

$$A(x) = \sum_{j=0}^{n-1} b_j (x - x_0)^j \ ,$$

   montrer comment calculer $A^{(k)}(x_0)$ pour tous les $k \in \{0, 1, \ldots, n-1\}$ en temps $O(n)$.

2. Expliquer comment trouver les b_i de l'équation ci-dessus en temps $O(n \log n)$, connaissant $A(x_0 + \omega_n^k)$ pour $k \in \{0, 1, \ldots, n-1\}$.

3. Démontrer que

$$A(x_0 + \omega_n^k) = \sum_{r=0}^{n-1} \left(\frac{\omega_n^{kr}}{r!} \sum_{j=r}^{n-1} f(j) g(j-r) \right) \ ,$$

   où $f(j) = a_j j!$ et $g(l) = x_0^l / (l!)$.

4. Expliquer comment évaluer $A(x_0 + \omega_n^k)$ pour $k \in \{0, 1, \ldots, n-1\}$ en temps $O(n \log n)$. (*Indication:* on pourra appliquer plusieurs FFT)

5. Conclure.

2 Borne inférieure de complexité

Definition 1 Un *calcul arithmétique* sur un corps K à partir d'un ensemble de paramètres $\{a_1, \ldots, a_n\}$ est une suite d'instructions de type :

$$f_1 \leftarrow o_1 \ \mathsf{op_1} \ o'_1; f_2 \leftarrow o_2 \ \mathsf{op_2} \ o'_2; \ldots; f_k \leftarrow o_k \ \mathsf{op_k} \ o'_k;$$

où pour tout $1 \leq i \leq k$, f_i est une variable du calcul, $\mathsf{op_i} \in \{+, -, \times\}$ et les opérandes o_i, o'_i sont soit des élements de K soit des paramètres soit l'une des variables $\{f_1, \ldots, f_{i-1}\}$.

Le programme ci-dessous calcule le produit de deux nombres complexes $(a+ib)(c+id)$ (le résultat est $f_3 + if_6$). Ici les paramètres sont a, b, c, d.

$f_1 \leftarrow a \times c; f_2 \leftarrow b \times d; f_3 \leftarrow f_1 - f_2; f_4 \leftarrow a \times d; f_5 \leftarrow b \times c; f_6 \leftarrow f_4 + f_5;$

Exercice 2 Proposez un calcul de ce produit qui n'utilise que 3 multiplications.

Exercice 3 Soit un calcul qui renvoie r résultats et qui comprend s multiplications. Montrez que le vecteur des résultats, noté $\mathbf{v}$, vérifie $\mathbf{v} = \mathbf{Me} + \mathbf{h}$ où $\mathbf{M}$ est une matrice $r \times s$ à valeurs dans K, $\mathbf{e}$ est un vecteur de dimension s à valeurs dans $\mathsf{K}[a_1, \ldots, a_n]$ (l'anneau des polynômes dont les variables sont $a_1, \ldots, a_n$) et $\mathbf{h}$ est un vecteur de dimension r dont les coefficients sont de la forme $c_0 + \sum_{i=1}^{n} c_i a_i$ avec $c_i \in \mathsf{K}$ pour tout i.

Definition 2 Soit $\mathbf{v}_1, \ldots, \mathbf{v}_m$ des vecteurs de dimension r à coefficients dans $\mathsf{K}[a_1, \ldots, a_n]$, on dit que $\mathbf{v}_1, \ldots, \mathbf{v}_m$ sont *linéairement indépendants modulo* K si :

$$\forall c_1, \ldots, c_m \in \mathsf{K},\ \sum_{i=1}^{m} c_i \mathbf{v}_i \in \mathsf{K}^r \Rightarrow \forall 1 \leq i \leq m, c_i = 0$$

Le *rang ligne (resp. colonne) modulo* K d'une matrice à coefficients dans $\mathsf{K}[a_1, \ldots, a_n]$ est le nombre maximal de vecteurs lignes (colonnes) linéairement indépendants modulo K.

Exercice 4 Soit un calcul dont les paramètres sont $a_1, \ldots, a_n, x_1, \ldots, x_p$. Ce calcul effectue le produit matrice-vecteur $\mathbf{Ax}$ où $\mathbf{A}$ est une matrice $r \times p$ à coefficients dans $\mathsf{K}[a_1, \ldots, a_n]$ et $\mathbf{x} = (x_1, \ldots, x_p)$. Montrez que le nombre de multiplications de ce calcul est au moins r si $\mathbf{A}$ est de rang ligne r modulo K.

Exercice 5 En déduire qu'un calcul de $ac, bd, ad + bc$ requiert au moins trois multiplications.

Exercice 6 Soit $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ un ensemble de vecteurs de dimension r à coefficients dans $\mathsf{K}[a_1, \ldots, a_n]$ contenant q vecteurs linéairement indépendants modulo K. Montrez que pour tout $b_2, \ldots, b_m \in \mathsf{K}$, l'ensemble $\{\mathbf{v}_2 + b_2\mathbf{v}_1, \ldots, \mathbf{v}_m + b_m\mathbf{v}_1\}$ contient $q-1$ vecteurs linéairement indépendants modulo K.

Soit un calcul dont les paramètres sont $a_1, \ldots, a_n, x_1, \ldots, x_p$. Ce calcul effectue le produit matrice-vecteur $\mathbf{Ax} + \mathbf{y}$ où $\mathbf{A}$ est une matrice $r \times p$ à coefficients dans $\mathsf{K}[a_1, \ldots, a_n]$, $\mathbf{x} = (x_1, \ldots, x_p)$ et $\mathbf{y} = (y_1, \ldots, y_r)$ avec les $y_1, \ldots, y_r \in \mathsf{K}[a_1, \ldots, a_n]$. Une multiplication de ce calcul est dite *active* si l'une des opérandes contient un x_i et l'autre opérande n'est pas un élément de K.

Exercice 7 Montrez que le nombre de multiplications actives d'un tel calcul est au moins égal au rang colonne modulo K de $\mathbf{A}$. Procédez par récurrence sur le rang colonne.

Exercice 8 En déduire qu'un calcul du produit d'une matrice $n \times p$ par un vecteur de dimension p où les paramètres sont les coefficients de la matrice et du vecteur requiert au moins np multiplications.