1 Transformée de Fourrier rapide : évaluation et multiplication de polynômes

Soit $\mathbb{C}[X]$ l'ensemble des polynômes à coefficients dans $\mathbb{C}$. Un polynôme $P(X) = \sum_{0 \leqslant i < n} a_i X^i \in \mathbb{C}[X]$ est représenté par le vecteur $[a_0, \cdots, a_{n-1}]$ de ses coefficients ($\forall i \in \{0, \cdots, n-1\}, a_i \in \mathbb{C}$).

On rappelle le théorème suivant :

Theorem 1. *Soit $P(X) \in \mathbb{C}[X]$ de degré au plus $n \in \mathbb{N}$ et soient $(x_0, \cdots, x_n) \in \mathbb{C}^{n+1}$ des complexes deux-à-deux distincts. Alors $P(X) = 0$ (le polynôme nul) si et seulement si $P(x_i) = 0$ pour tout $i \leqslant n$.*

On étudie ici une méthode pour multiplier rapidement deux polynômes. On transforme les données du problème (deux polynômes) en objets faciles à manipuler (des racines de l'unité) sur lesquels on effectue l'opération considérée puis on effectue la transformation inverse sur le résultat obtenu. Par complexité (temporelle), on désigne une estimation ("grand O") du nombre d'opérations élémentaires : multiplication, division, addition et soustraction de nombres complexes. Le parcours d'un vecteur de longueur $n \in \mathbb{N}$ est $O(n)$.

1.1 Préliminaires

Soient $p \in \mathbb{N}^*$ et $n = 2^p$. Soit $P \in \mathbb{C}[X]$ représenté par le vecteur $[a_0, \cdots, a_n]$.

Question 1	Prouver qu'il existe une unique paire $(A(X), B(X)) \in \mathbb{C}[X]^2$ de polynômes de degré $\leqslant n/2$ tels que $P(X) = X^{n/2}A(X) + B(X)$.

Question 2	Donner les représentations des polynômes A et B tels que $P(X) = X^{n/2}A(X) + B(X)$. Quelle est la complexité du calcul des représentations des polynômes A et B en fonction de la représentation de P ?

Algorithm 1 Méthode de Horner

Require: polynôme $P(X) = \sum_{0 \leqslant i \leqslant n} a_i X^i \in \mathbb{C}[X]$ et $x \in \mathbb{C}$

```
z ← a_n
for i = n − 1 à 0 do
    z ← a_i + x ∗ z
return z
```

Question 3	On considère l'algorithme 1 (méthode de Horner). – Expliquer ce qu'il calcule. – Prouver sa correction. – Donner sa complexité en fonction du degré $n \geqslant 0$ du polynôme.

1.2 Méthode de Karatsuba

Soient $P, Q \in \mathbb{C}[X]$ de degré au plus $n = 2^p$. Soient A, B, C et D les quatre polynômes de degré au plus $n/2$ tels que $P(X) = X^{n/2}A(X) + B(X)$ et $Q(X) = X^{n/2}C(X) + D(X)$. On rappelle ici que la méthode de Karatsuba pour multiplier deux polynômes P et Q utilise le fait que

$$P(X)Q(X) = X^n(A(X)C(X)) + X^{n/2}((A(X) + B(X))(C(X) + D(X)) - A(X)C(X) - B(X)D(X)) + B(X)D(X).$$

Soit $c(p)$ le nombre d'opérations élémentaires pour calculer le produit de deux polynômes de degré $n = 2^p$ par la méthode de Karatsuba.

Question 4	Exprimer $c(p)$ en fonction de $c(p-1)$. En déduire $c(p)$ (sans preuve).

1.3 Alternative pour la représentation de polynômes

Soit $n \in \mathbb{N}$. Soient $n+1$ nombres complexes $Y = (y_0, \cdots, y_n) \in \mathbb{C}^{n+1}$ deux-à-deux distincts. Soient P et $Q \in \mathbb{C}[X]$ de degré au plus n.

Question 5	Prouver que $P = Q$ si et seulement si P et Q ont même degré et $P(y_i) = Q(y_i)$ pour tout $0 \leqslant i \leqslant n$.

D'après la question précédente, un polynôme P de degré $n \geqslant 0$ est uniquement défini par ses valeurs en $n+1$ points distincts, c'est-à-dire que, pour tout $Y = (y_0, \cdots, y_n) \in \mathbb{C}^{n+1}$ et, pour tout $0 \leqslant i, j \leqslant n$, $y_i = y_j \Leftrightarrow i = j$, P est uniquement défini par $P\{Y\} = (P(y_0), \cdots, P(y_n))$.

Question 6	Proposer un algorithme qui calcule $P.Q\{Y\}$ en fonction de $P\{Y\}$ et $Q\{Y\}$ en $O(n)$ opérations élémentaires.

Soit $Y \in \mathbb{C}^{n+1}$. Soient $f : \mathbb{N} \to \mathbb{N}$ et $g : \mathbb{N} \to \mathbb{N}$. Supposons qu'il existe un algorithme $\mathcal{A}_1$ qui permet de calculer $P\{Y\}$ en fonction de a en temps $f(n)$ et un algorithme $\mathcal{A}_2$ qui permet de calculer a en fonction de $P\{Y\}$ en temps $g(n)$, pour tout polynôme $P(X) = \sum_{0 \leqslant i \leqslant m} a_i X^i \in \mathbb{C}[X]$, représenté par le vecteur $a = [a_0, \cdots, a_m]$ avec $m \leqslant n$.

Question 7	Soient $P(X) = \sum_{0 \leqslant i \leqslant n/2} a_i X^i \in \mathbb{C}[X]$ et $Q(X) = \sum_{0 \leqslant i \leqslant n/2} b_i X^i \in \mathbb{C}[X]$. Proposer un algorithme qui calcule $P.Q(X) = \sum_{0 \leqslant i \leqslant n} c_i X^i$ en temps $O(f(n) + g(n) + n)$.

Question 8	Quels doivent être les ordres de grandeur de f et g pour que l'algorithme précédent soit plus efficace que l'algorithme de Karatsuba ?

Dans la suite, on explique comment concevoir les algorithmes $\mathcal{A}_1$ et $\mathcal{A}_2$ pour "battre" l'algorithme de Karatsuba. Plus précisemment, en choisissant astucieusement $Y \in \mathbb{C}^{n+1}$, pour tout polynôme $P(X) = \sum_{0 \leqslant i < \leqslant n} a_i X^i \in \mathbb{C}[X]$, il est possible de "passer" efficacement des coefficients $[a_0, \cdots, a_n]$ à $P\{Y\}$ et réciproquement.

1.4 Transformée de Fourrier

Soit $p \in \mathbb{N}$ et $n = 2^p$. Soit $Y = (y_0, \cdots, y_{n-1})$ la suite des racines n-ièmes de l'unité, c'est-à-dire $y_k = e^{2ik\pi/n}$, $k < n$. Soit $Z = (z_0, \cdots, z_{n-1}) \in \mathbb{C}^n$ et soit $P \in \mathbb{C}[X]$ le polynôme de degré $< n$ tel que $P\{Y\} = Z$. Soit $Z_0 = (z_0, z_2, z_4, \cdots, z_{n-2})$ et $Z_1 = (z_1, z_3, \cdots, z_{n-1})$. Soit $Y_0 = (y_0, y_2, y_4, \cdots, y_{n-2})$ et $Y_1 = (y_1, y_3, \cdots, y_{n-1})$. Soient P_0 et $P_1 \in \mathbb{C}[X]$ de degré $< 2^{p-1} = n/2$ tels que $P_0\{Y_0\} = Z_0$ et $P_1\{Y_0\} = Z_1$.

Pour la question suivante, on rappelle que $y_k^{n/2} = 1$ si k est pair et $y_k^{n/2} = -1$ sinon.

Question 9	Prouver que, pour tout $x \in \mathbb{C}$, $P(x) = \frac{1+x^{n/2}}{2} P_0(x) + \frac{1-x^{n/2}}{2} P_1(e^{-2i\pi/n} x)$.

Question 10	Donner un algorithme qui calcule les coefficients de P en fonction des coefficients de P_0 et P_1.

Question 11	En déduire un algorithme **récursif** qui calcule les coefficients de P en fonction de $P\{Y\} = Z$. Donner la complexité $c(p)$ de cet algorithme en fonction de p.

Ainsi, il est possible de passer efficacement de la représentation $P\{Y\} = Z$ d'un polynôme $P(X) = \sum_{0 \leqslant i < n} a_i X^i \in \mathbb{C}[X]$ à celle de ses coefficients.

Soit $P(X) = \sum_{0 \leqslant i < n} a_i X^i \in \mathbb{C}[X]$. On pose $Q_0(X) = \sum_{0 \leqslant i < n/2} a_{2i} X^i$ et $Q_1(X) = \sum_{0 \leqslant i < n/2} a_{2i+1} X^i$.

Question 12	Prouver que, pour tout $x \in \mathbb{C}$, $P(x) = Q_0(x^2) + x \cdot Q_1(x^2)$.

Question 13	Soit $Y \in \mathbb{C}^n$ la suite des racines n-ièmes de l'unité. Proposer un algorithme qui calcule $P\{Y\}$ en fonction des coefficients de P de degré $< n = 2^p$, en temps $O(n \log n)$.

Question 14	Déduire des questions précédentes un algorithme pour multiplier deux polynômes de degré $< n$. Donner sa complexité et comparer avec la méthode de Karatsuba.