Préparation aux oraux CCINP n°2

Polynômes

Soient P et Q deux polynômes de degré inférieur ou égal à $2n-1$. Soient P_0, Q_0, P_1, et Q_1 quatre polynômes de degré inférieurs ou égaux à $n-1$ tels que

$$P = P_0 + X^n P_1 \quad \text{et} \quad Q = Q_0 + X^n Q_1.$$

On remarque que

$$\begin{aligned} P \times Q &= P_0 Q_0 + X^n (P_1 Q_0 + P_0 Q_1) + X^{2n} P_1 Q_1 \\ &= P_0 Q_0 + X^n ((P_0 + P_1)(Q_0 + Q_1) - P_0 Q_0 - P_1 Q_1) + X^{2n} P_1 Q_1 \end{aligned}$$

Q1. En déduire un algorithme « *diviser pour régner* » calculant $P \times Q$ utilisant les fonctions :

- $\text{degré}(P)$ donne le degré de P ;
- $\text{ajout}(P, Q)$ (resp. $\text{soustrait}(P, Q)$) calcule $P + Q$ (resp. $P - Q$) ;
- $\text{décale}(P, n)$ calcule $X^n \times P$;
- $\text{découpe}(P, n)$ calcule P_0 et P_1 de degrés inférieurs ou égaux à $n-1$ tels que l'égalité polynomiale $P = P_0 + X^n P_1$ soit vérifiée.
- $\text{produit\_degré\_1}(P, Q)$ calcule $P \times Q$ lorsque P et Q sont de degrés inférieurs ou égaux à 1.

On pourra supposer P et Q de même degré.

Q2. On note $C(n)$ le coût de cet algorithme lorsque P et Q sont représentés par des listes de taille n.

(1) Montrer que $C(n) \leq 3C\left(\frac{n}{2}\right) + Kn$, où K est un entier indépendant des entrées et de n.

(2) On étudie le cas où $n = 2^p$, pour $p \in \mathbb{N}$. Chercher α minimal tel que $C(n) = \mathrm{O}(n^\alpha)$. (On se contentera d'exhiber un tel α sans montrer son caractère minimal.)

(3) Expliquer comment faire dans le cas où n est quelconque.

Q3. On s'intéresse maintenant au calcul de Q^k, pour un polynôme Q de degré n donné.

(1) Remarquons que $Q^{k+1} = Q \times Q^k$ et que $Q^0 = 1$. En utilisant cette remarque et l'algorithme de Q1, écrire un algorithme permettant de calculer Q^k.

(2) Quelle est la complexité de cet algorithme ?

(3) En utilisant une stratégie « *diviser pour régner* », proposer un algorithme ayant une meilleur complexité.

Hugo Salou