Université Bordeaux 1 | **Algèbre et calcul formel – Master**
Mathématiques | Année 2012–2013

FEUILLE D'EXERCICES n° 4

Exercice 1 – [Divide and conquer, un exemple : Toom-Cook]

Soit R un polynôme de degré inférieur ou égal à 4. Q Combien de valeurs de R faut-il connaître pour pouvoir reconstituer R ?

1) On note $R = a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$, et $R(\infty) = a_4$.

2) Montrer l'égalité

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 16 & 8 & 4 & 2 & 1 \end{pmatrix} \begin{pmatrix} a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} R(\infty) \\ R(0) \\ R(1) \\ R(-1) \\ R(2) \end{pmatrix}.$$

3) En déduire l'égalité

$$\begin{pmatrix} a_4 \\ a_3 \\ a_2 \\ a_1 \\ a_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ -2 & \frac{1}{2} & -\frac{1}{2} & -\frac{1}{6} & \frac{1}{6} \\ -1 & -1 & \frac{1}{2} & \frac{1}{2} & 0 \\ 2 & -\frac{1}{2} & 1 & -\frac{1}{3} & -\frac{1}{6} \\ 0 & 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} R(\infty) \\ R(0) \\ R(1) \\ R(-1) \\ R(2) \end{pmatrix}.$$

4) Soient $P = 3X^2 + X - 1$, $Q = X^2 - 2X + 1$ et $R = PQ$. Calculer $R(\infty)$, $R(0)$, $R(1)$, $R(-1)$ et $R(2)$, puis reconstituer R en utilisant la question précédente.

5) Il aurait été plus simple de calculer R en multipliant P et Q de façon classique, mais un traitement récursif de cette méthode donne un algorithme plus efficace quand les degrés de P et de Q sont grands.

On suppose que P et Q sont des polynômes de $\mathbb{C}[X]$ de degrés strictement inférieur à $n = 3^r$. On note

$$P = \sum_{i=0}^{n-1} a_i X^i \quad \text{et } Q = \sum_{i=0}^{n-1} b_i X^i.$$

Expliquer ce que fait l'algorithme *Toom-Cook* suivant.

Dans cet algorithme, on note *Interp*$(z_1, \ldots, z_5, Y)$ le polynôme R en la variable Y de degré inférieur ou égal à 4 dont les valeurs en $y_1 = \infty$, $y_2 = 0$, $y_3 = 1$, $y_4 = -1$ et $y_5 = 2$ sont $(z_1, \ldots, z_5)$.

Toom-Cook(P, Q, n) :

(1) Si $n = 1$, retourner PQ.

(2) Écrire P et Q sous la forme

$$P = (X^{n/3})^2 P_2 + X^{n/3} P_1 + P_0 \quad \text{et} \quad Q = (X^{n/3})^2 Q_2 + (X^{n/3})^2 Q_1 + Q_0,$$

où les P_i et les Q_j sont des polynômes de degrés inférieurs strictement à $n/3$.

(3) Soient les polynômes de $\mathbb{C}[X][Y]$

$$A = Y^2 P_2 + Y P_1 + P_0 \quad \text{et} \quad B = Y^2 Q_2 + Y Q_1 + Q_0.$$

(4) Pour i de 1 à 5, faire $z_i =$*Toom-Cook*$(A(y_i), B(y_i), n/3)$ (les z_i sont alors des polynômes en X).

(5) *Produit* =*Interp*$(z_1, z_2, z_3, z_4, z_5, Y)$.

(6) Retourner $R =$ *Produit*$(X^{n/3})$

6) Y a-t-il un lien entre cet algorithme et l'algorithme de Karatsuba ?

7) Quelle est la complexité de l'algorithme Toom-Cook ?

Exercice 2 – [DIVIDE AND CONQUER : UNE GÉNÉRALISATION DU LEMME FONDAMENTAL]

On rappelle le lemme pratique qui permet de calculer plus facilement la complexité si l'on utilise une approche du type "divide and conquer".

Lemme. *Soit $f : \mathbb{R}^+ \to \mathbb{R}^+$ telle que*

- *f est bornée sur $[0, 1)$;*
- *quel que soit $x \geqslant 1$, on a $f(x) \leqslant af(x/b) + Mx$ où a, $M > 0$ et $b > 1$.*

Alors sur $[1, \infty)$ on a

$$f(x) = \begin{cases} O(x^{\log a/\log b}) & si \quad a > b \\ O(x \log x) & si \quad a = b \\ O(x) & si \quad a < b \end{cases}$$

À l'aide d'un changement de variable approprié, établir la généralisation suivante.

Lemme bis. *Soit $f : \mathbb{R}^+ \to \mathbb{R}^+$ telle que*

- *f est bornée sur $[0, 1)$;*
- *quel que soit $x \geqslant 1$, on a $f(x) \leqslant af(x/b) + Mx^r$ où a, M, $r > 0$ et $b > 1$.*

Alors sur $[1, \infty)$ on a

$$f(x) = \begin{cases} O(x^{\log a/\log b}) & si \quad a > b^r \\ O(x^r \log x) & si \quad a = b^r \\ O(x^r) & si \quad a < b^r \end{cases}$$

Exercice 3 – [DIVIDE AND CONQUER, UN AUTRE EXEMPLE : STRASSEN]
Soient A et B deux matrices $n \times n$. On cherche à calculer $C = AB$ de façon économique. On suppose pour commencer (questions 1 à 5) que n est une puissance de 2. On divise A, B et C en 4 matrices $n/2 \times n/2$.

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix} \quad \text{et} \quad C = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \end{pmatrix}.$$

On pose

$$\begin{cases} P_1 & = & A_1(B_2 - B_4) \\ P_2 & = & (A_1 + A_2)B_4 \\ P_3 & = & (A_3 + A_4)B_1 \\ P_4 & = & A_4(B_3 - B_1) \\ P_5 & = & (A_1 + A_4)(B_1 + B_4) \\ P_6 & = & (A_2 - A_4)(B_3 + B_4) \\ P_7 & = & (A_1 - A_3)(B_1 + B_2) \end{cases}$$

1) Exprimer C_2 à l'aide de P_1 et P_2, C_3 à l'aide de P_3 et P_4, C_1 à l'aide de $P_4 + P_5$ et $P_2 - P_6$ et C_4 à l'aide de $P_1 + P_5$ et $P_3 + P_7$.

2) En déduire le nombre de sommes et de multiplications de matrices $n/2 \times n/2$ suffisant au calcul de C par la méthode préconisée.

3) Calculer le nombre total de mutiplications que l'on est amené à faire dans l'algorithme défini en itérant le processus.

4) Exprimer la relation de récurrence que vérifie la complexité algébrique c_n de l'algorithme.

5) Montrer que l'on a

$$c_n = O\left(n^{\log 7/\log 2}\right).$$

6) Généraliser à n quelconque.

7) Comparer avec la complexité de l'algorithme naïf issu de l'application directe de la formule

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Exercice 4 – [DIVISION COMPLEXE]
Soient deux nombres complexes $z_1 = a_0 + a_1 i$ et $z_2 = b_0 + b_1 i \neq 0$. Peut-on évaluer les parties réelle et imaginaire du quotient z_1/z_2 en effectuant au plus 7 multiplications et divisions dans $\mathbb{R}$? Peut-on le faire en effectuant au plus 6 multiplications et divisions dans $\mathbb{R}$?