

## TD5 : Borne de complexité et FFT

### 1 Borne inférieure de complexité

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

$$f_1 \leftarrow o_1 \text{ op}_1 o'_1; f_2 \leftarrow o_2 \text{ op}_2 o'_2; \dots; f_k \leftarrow o_k \text{ op}_k o'_k;$$

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

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  $a, b, c, d$ .

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

**Question 1 :** Proposer un calcul de ce produit qui n'utilise que 3 multiplications.

**Question 2 :** Soit un calcul qui renvoie  $r$  résultats et qui comprend  $s$  multiplications. Montrer que le vecteur des résultats, noté  $\mathbf{v}$ , vérifie  $\mathbf{v} = \mathbf{M}\mathbf{e} + \mathbf{h}$  où  $\mathbf{M}$  est une matrice  $r \times s$  à valeurs dans  $\mathbb{K}$ ,  $\mathbf{e}$  est un vecteur de dimension  $s$  à valeurs dans  $\mathbb{K}[a_1, \dots, a_n]$  (l'anneau des polynômes dont les variables sont  $a_1, \dots, a_n$ ) 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  $c_i \in \mathbb{K}$  pour tout  $i$ .

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

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

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

**Question 3 :** Soit un calcul dont les paramètres sont  $a_1, \dots, a_n, x_1, \dots, x_p$ . Ce calcul effectue le produit matrice-vecteur  $\mathbf{A}\mathbf{x}$  où  $\mathbf{A}$  est une matrice  $r \times p$  à coefficients dans  $\mathbb{K}[a_1, \dots, a_n]$  et  $\mathbf{x} = (x_1, \dots, x_p)$ . On souhaite montrer que le nombre de multiplications de ce calcul est au moins  $r$  (dans le pire des cas). On suppose par l'absurde que le rang ligne modulo  $\mathbb{K}$  vaut  $r$  et qu'il est strictement supérieur au nombre de multiplications noté  $s$ .

1. Montrer qu'il existe  $\mathbf{y}$  à coefficients dans  $\mathbb{K}$  non tous nuls, et  $\mathbf{h}$  à coefficients de la forme  $c_0 + \sum_{i=1}^n c_i a_i + \sum_{i=1}^p c'_i x_i$  tels que  $\mathbf{y}^T \mathbf{A}\mathbf{x} = \mathbf{y}^T \mathbf{h}$ .
2. Montrer que  $\mathbf{y}^T \mathbf{A}$  est un vecteur ligne à valeurs dans  $\mathbb{K}$ . (hint :  $\mathbf{y}^T \mathbf{A}$  est à coefficients dans  $\mathbb{K}[a_1 \dots a_n]$  alors que  $\mathbf{x} = (x_1 \dots x_p)$ ).
3. En déduire que l'hypothèse était absurde : le nombre de multiplications de ce calcul est au moins égal au rang ligne modulo  $\mathbb{K}$  de  $\mathbf{A}$ .

**Question 4 :** En déduire qu'un calcul de  $ac, bd, ad + bc$  requiert au moins trois multiplications.

**Question 5 :** Soit  $\{\mathbf{v}_1, \dots, \mathbf{v}_m\}$  un ensemble de vecteurs de dimension  $r$  à coefficients dans  $\mathbb{K}[a_1, \dots, a_n]$  contenant  $q$  vecteurs linéairement indépendants modulo  $\mathbb{K}$ . On considère les vecteurs  $\mathbf{v}'_i = \mathbf{v}_i + b_i \mathbf{v}_1$  pour  $i \in [2; m]$  où  $b_i \in \mathbb{K}$ . On souhaite montrer qu'il existe  $q - 1$  vecteurs  $\mathbf{v}'_i$  linéairement indépendants modulo  $\mathbb{K}$ .

1. Conclure dans le cas où  $\{\mathbf{v}_1, \dots, \mathbf{v}_q\}$  sont linéairement indépendants modulo  $\mathbb{K}$ . On suppose désormais (quite à réordonner) que  $\{\mathbf{v}_2, \dots, \mathbf{v}_{q+1}\}$  sont linéairement indépendants modulo  $\mathbb{K}$ .

2. On suppose (par l'absurde) que ni  $\{\mathbf{v}'_2 \dots \mathbf{v}'_q\}$  ni  $\{\mathbf{v}'_3 \dots \mathbf{v}'_{q+1}\}$  ne sont linéairement indépendants modulo  $\mathbb{K}$ . Montrer qu'il existe  $c_1 \dots c_q$  dans  $\mathbb{K}$  tels que  $\sum_{i=1}^q c_i \mathbf{v}_i = \mathbf{w} \in \mathbb{K}^r$  ainsi que  $c_1 \neq 0$  et  $c_2 \dots c_q$  non tous nuls. On suppose dans la suite  $c_2 \neq 0$  (quitte à réordonner). En déduire de même qu'il existe  $\mathbf{z} \in \mathbb{K}^r$  et  $d_1 \neq 0$ , ainsi que  $d_3 \dots d_{q+1}$  non tous nuls tels que  $d_1 \mathbf{v}_1 + \sum_{i=3}^{q+1} d_i \mathbf{v}_i = \mathbf{z}$
3. Exprimer  $d_1 \mathbf{w} - c_1 \mathbf{z}$  à l'aide des  $c_i, d_i$  afin d'obtenir une contradiction.

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

**Question 6 :** Montrer que le nombre de multiplications actives d'un tel calcul est au moins égal au rang colonne modulo  $\mathbb{K}$  de  $\mathbf{A}$ . *Indication :* Procéder par récurrence sur le rang colonne modulo  $\mathbb{K}$ .

**Question 7 :** 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.

## 2 Forme Normale Algébrique d'une fonction booléenne

On s'intéresse à une fonction booléenne  $f : \{0, 1\}^n \mapsto \{0, 1\}$ . On note  $\mathbb{B} = \{0, 1\}$ . Cette fonction peut être représentée par sa table de vérité ou bien comme un polynôme à plusieurs variables de degré au plus  $n$  sur  $\mathbb{B}[x_1, \dots, x_n]$ . On rappelle que sur le corps  $\mathbb{B}$ , l'addition est le **xor** et la multiplication est le **and**.

**Question 1 :** Montrer que  $f$  s'écrit :  $f(x_1, \dots, x_n) = \sum_{(a_1, \dots, a_n) \in \mathbb{B}^n} g(a_1, \dots, a_n) \cdot x_1^{a_1} \dots x_n^{a_n}$  où  $g : \mathbb{B}^n \mapsto \mathbb{B}$ . Cette représentation est la Forme Normale Algébrique (FNA) de  $f$ .

**Question 2 :** Exprimer  $g$  dans le cas où  $n = 1$ . Montrez que la procédure qui calcule  $g$  en fonction de  $f$  est *involutive*, c'est à dire qu'elle permet aussi de calculer  $f$  en fonction de  $g$ .

**Question 3 :** Montrer que  $f$  peut s'écrire sous la forme  $f(x_1, \dots, x_n) = f_0(x_1, \dots, x_{n-1}) + x_n \cdot f_1(x_1, \dots, x_{n-1})$ .

**Question 4 :** Soit  $g_0$  et  $g_1$  les FNA de  $f_0$  et  $f_1$  respectivement. Exprimer  $g$  en fonction de  $g_0$  et  $g_1$ .

**Question 5 :** En déduire un algorithme de calcul de  $g$  et donner sa complexité.

## 3 Application de FFT : filtrage

**Question 1 :** Un dispositif physique tel qu'un microphone, un oscilloscope, etc. est utilisé pour acquérir constitué par une suite de réels  $x_0, \dots, x_n$  assez longue. Lorsque le dispositif n'est pas de très bonne qualité et que les échantillons contiennent du "bruit", une mesure rudimentaire pour lutter contre ce phénomène consiste à appliquer un lissage gaussien, c'est à dire à remplacer chaque échantillon par une moyenne pondérée de ses voisins :

$$y_i = \frac{1}{Z} \sum_{j=-k}^k x_{i+j} \cdot e^{-j^2}$$

où  $k$  est un paramètre de largeur et  $Z$  un facteur de normalisation choisi convenablement. On remarque qu'il y a un problème pour les valeurs limites, mais il est résolu en ne calculant ni les  $k$  premières valeurs, ni les  $k$  dernières. Montrer comment calculer  $y$  en temps  $\mathcal{O}(n \log n)$ .