TD 5 :
Bornes inférieures de complexité en calcul formel

1 Bornes inférieures de complexité en calcul arithmétique

Définition 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 éléments de* K*, soit des paramètres, soit l'une des variables* $\{f_1, \ldots, f_{k-1}\}$.

Le programme ci-dessous calcule le produit de deux nombres complexes $(a + ib)(c + id)$; le résultat est $f_3 + if_6$ et 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 arithmétique qui renvoie r résultats et qui comprend s multiplications. Montrer 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.

Définition 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 :*

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

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

Question 3 : Soit le calcul arithmétique qui 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 $\mathbf{x} = (x_1, \ldots, x_p)$. Les paramètres de ce calcul sont $a_1, \ldots, a_n, x_1, \ldots, x_p$. On souhaite montrer que le nombre de multiplications de ce calcul est au moins r pour le pire des cas (pas de 0 dans $\mathbf{A}$). Pour cela, on suppose par l'absurde que le rang ligne modulo K de A vaut r et que $r > s$, où s est le nombre de multiplications du calcul.

1. Montrer qu'il existe $\mathbf{y}$ à coefficients dans K différent de $\mathbf{0}$, 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 $\mathbf{y}^T \mathbf{Ax} = \mathbf{y}^T \mathbf{h}$.
2. Montrer que $\mathbf{y}^T \mathbf{A}$ est un vecteur ligne à valeurs dans K.
3. En déduire que l'hypothèse était absurde : le nombre de multiplications de ce calcul est au moins égal au rang ligne modulo K de $\mathbf{A}$.

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

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

1. Conclure dans le cas où $\{\mathbf{v}_1, \ldots, \mathbf{v}_q\}$ sont linéairement indépendants modulo K.
   On suppose désormais (quitte à réordonner) que $\{\mathbf{v}_2, \ldots, \mathbf{v}_{q+1}\}$ sont linéairement indépendants modulo K, c'est à dire $\mathbf{v}_1$ n'est pas dans les q vecteurs linéairement indépendants.
2. On suppose (par l'absurde) que les deux ensembles $\{\mathbf{v}'_2, \ldots, \mathbf{v}'_q\}$ et $\{\mathbf{v}'_3, \ldots, \mathbf{v}'_{q+1}\}$ sont linéairement dépendants modulo K. Montrer qu'il existe $c_1, \ldots, c_q$ dans K tels que $\sum_{i=1}^{q} c_i\mathbf{v}_i = \mathbf{w} \in \mathsf{K}^r$ ainsi que $c_1 \neq 0$ et $c_2, \ldots, c_q$ non tous nuls. On suppose dans la suite $c_2 \neq 0$ (quitte à réordonner). En déduire de même qu'il existe $\mathbf{z} \in \mathsf{K}^r$ et $d_1 \neq 0$, ainsi que $d_3, \ldots, d_{q+1}$ 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 le calcul arithmétique qui 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 $\mathbf{y} = (y_1, \ldots, y_r) \in \mathsf{K}^r[a_1, \ldots, a_n]$. Les paramètres de ce calcul sont $a_1, \ldots, a_n, x_1, \ldots, x_p$. 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.

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

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 $f : \{0, 1\}^n \to \{0, 1\}$. 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 $\mathbb{B}[x_1, \ldots, x_n]$. On rappelle que sur le corps $\mathbb{B}$, l'addition est le `xor`, la multiplication est le `and` et $x^0 = 1$.

Question 8 : Montrer que f s'écrit : $f(x_1, \ldots, x_n) = \sum_{(a_1,\ldots,a_n)\in\mathbb{B}^n} g(a_1, \ldots, a_n) \cdot x_1^{a_1} \cdots x_n^{a_n}$ où $g : \mathbb{B}^n \to \mathbb{B}$. Cette représentation est la Forme Normale Algébrique (FNA) de f.

Question 9 : 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 10 : Montrer que f peut s'écrire sous la forme $f(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1}) + x_n \cdot f_1(x_1, \ldots, x_{n-1})$.

Question 11 : Soit g_0 et g_1 les FNA de f_0 respectivement f_1. Exprimer g en fonction de g_0 et g_1.

Question 12 : (DM) En déduire un algorithme de calcul de g et donner sa complexité.