TD 5 :
Bornes inférieures de complexité en calcul formel

Correction

1 Bornes inférieures de complexité en calcul arithmétique

Question 1 : Correction : On a $(a+ib)(c+id) = (ac-bd)+(ad+bc)i$. Un calcul utilisant que trois multiplications repose sur les identités :

$$ad + bc = (a+b)c + a(d-c) \tag{1}$$
$$ac - bd = (a+b)c - b(c+d) \tag{2}$$

Le calcul obtenu est donné ci-dessous et le résultat est $f_8 + if_5$:

$$f_1 \leftarrow a+b; f_2 \leftarrow c \times f_1;\ f_3 \leftarrow d-c; f_4 \leftarrow a \times f_3; f_5 \leftarrow f_2 + f_4; \tag{3}$$
$$f_6 \leftarrow c+d; f_7 \leftarrow b \times f_6; f_8 \leftarrow f_2 - f_7; \tag{4}$$

Question 2 : Correction : L'exemple en introduction (à quatre multiplications) peut être écrit sur la forme :

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} a \times c \\ b \times d \\ a \times d \\ b \times c \end{bmatrix}$$

Le calcul avec trois multiplications s'écrit $\mathbf{Me} + \mathbf{h}$:

$$\begin{bmatrix} f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \\ f_8 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & -1 \end{bmatrix} \begin{bmatrix} c \times (a+b) \\ a \times (d-c) \\ b \times (c+d) \end{bmatrix} + \begin{bmatrix} a+b \\ 0 \\ d-c \\ 0 \\ 0 \\ c+d \\ 0 \\ 0 \end{bmatrix}$$

On remarque que chaque f_i est dans $\mathsf{K}[a_1, \ldots, a_n]$ car obtenu par addition, soustraction ou multiplication des termes dans $\mathsf{K}[a_1, \ldots, a_n]$. Donc si f_i est le résultat d'une multiplication, notons ceci $f_i^{\times}$, on introduit ce résultat dans $\mathbf{e}$ (disons ligne j), on assigne un 1 dans $\mathbf{M}$ (ligne i colonne j) et 0 en $\mathbf{h}$ (à la ligne i). Si f_i est le résultat d'une addition alors, on peut le réécrire en fonction des $f_j^{\times}$ précédents et des termes linéaires (car pas de multiplication entre paramètres), donc $f_i = \sum_{j<i,} c'_j f_j^{\times} + c_0 + \sum_{i=1}^{n} c_i a_i$.

Question 3 : Correction : (1) $\mathbf{Ax}$ est un calcul arithmétique sur $\mathsf{K}[a_1, \ldots, a_n, x_1, \ldots, x_p]$. Alors, d'après la question 2, $\mathbf{Ax}$ s'écrit sous la forme $\mathbf{Me} + \mathbf{h}$ avec :

— $\mathbf{M}$ de taille $r \times s$ avec coefficients en K,
— $\mathbf{e} \in \mathsf{K}^s[a_1, \ldots, a_n, x_1, \ldots, x_p]$,
— $\mathbf{h}$ un vecteur de r termes linéaires en $\mathsf{K}[a_1, \ldots, a_n, x_1, \ldots, x_p]$.

Si $r > s$ alors les lignes des $\mathbf{M}$ (en K^s) sont linéairement dépendantes, donc il existe un vecteur $\mathbf{y} \neq \mathbf{0}$ avec coefficients dans K tel que $\mathbf{y}^T\mathbf{M} = \mathbf{0}$.

Alors $\mathbf{y}^T\mathbf{A}\mathbf{x} = \mathbf{y}^T\mathbf{h}$ avec $\mathbf{h}$ un vecteur de r termes linéaires en $\mathsf{K}[a_1, \ldots, a_n, x_1, \ldots, x_p]$, donc s'écrivant $c_0 + \sum_{i=1}^{n} c_i a_i + \sum_{i=1}^{p} c'_i x_i$.

(2) Comme $\mathbf{y}^T\mathbf{A}\mathbf{x} = \mathbf{y}^T\mathbf{h}$ et $\mathbf{y}^T\mathbf{h}$ est linéaire en $\mathbf{x}$, alors $\mathbf{y}^T\mathbf{A}$ ne doit contenir que des constantes en $\mathbf{K}$, sinon on obtiendrait des monômes de degré au moins 2.

(3) Comme $\mathbf{y}^T\mathbf{A} \in \mathsf{K}^r$, alors les vecteurs lignes de $\mathbf{A}$ sont linéairement dépendantes, contradiction avec l'hypothèse que le rang ligne modulo K de $\mathbf{A}$ vaut r. Donc $r \leq s$.

Question 4 : Correction : Les trois calculs $ac, bd, ad + bc$ s'expriment comme le résultat d'un produit matrice avec un vecteur :

$$\begin{bmatrix} a & 0 \\ 0 & b \\ b & a \end{bmatrix} \times \begin{bmatrix} c \\ d \end{bmatrix}$$

On montre que le rang ligne modulo K (entiers) de la matrice est 3. Soit $c_1, c_2, c_3 \in \mathsf{K}$ et $\sum_{i=1}^{3} c_i \mathbf{v}_i \in \mathsf{K}^2$, avec $\mathbf{v}_1 = [a, 0]$, $\mathbf{v}_2 = [0, b]$, $\mathbf{v}_3 = [b, a]$. Donc $\begin{bmatrix} c_1 a + c_3 b \\ c_2 b + c_3 a \end{bmatrix} \in \mathsf{K}^2$ et comme $a, b \notin \mathsf{K}$, alors forcement $c_i = 0$. Il résulte que les lignes de la matrice sont linéairement indépendantes.

Question 5 : Correction : (1) Supposons que $\{\mathbf{v}_1, \ldots, \mathbf{v}_q\}$ sont linéairement indépendants modulo K. Regardons maintenant l'ensemble de vecteurs $\{\mathbf{v}'_2, \ldots, \mathbf{v}'_q\}$. Pour un tuple de valeurs $c_2, \ldots, c_q \in \mathsf{K}$, $\mathbf{w} = \sum_{i=2}^{q} c_i \mathbf{v}'_i = \sum_{i=2}^{q} c_i \mathbf{v}_i + \mathbf{v_1} \sum_{i=2}^{q} c_i b_i$. Or si $\mathbf{w} \in \mathsf{K}^r$ alors par l'hypothèse $c_i = 0$ pour $i \in [2, q]$ et $\sum_{i=2}^{q} c_i b_i = 0$. Donc les $q - 1$ vecteurs $\{\mathbf{v}'_2, \ldots, \mathbf{v}'_q\}$ sont linéairement indépendants.

(2) Si les $\mathbf{v}'_2, \ldots, \mathbf{v}'_q$ ou les $\mathbf{v}'_3, \ldots, \mathbf{v}'_{q+1}$ sont linéairement indépendants alors nous avons les $q - 1$ vecteurs $\mathbf{v}'_i$ linéairement indépendants. Considérons dans la suite le dernier cas, les DEUX ensembles sont des vecteurs linéairement dépendants.

Si $\mathbf{v}'_2, \ldots, \mathbf{v}'_q$ sont linéairement dépendants, il existe $c_2, \ldots, c_q \in \mathsf{K}$ non tous nuls tels que $\mathbf{w} = \sum_{i=2}^{q} c_i \mathbf{v}'_i \in \mathsf{K}^r$, avec $\mathbf{w} = \sum_{i=2}^{q} c_i \mathbf{v}_i + \mathbf{v_1} \sum_{i=2}^{q} c_i b_i \in \mathsf{K}^r$. Si $\sum_{i=2}^{q} c_i b_i = 0$ alors $\sum_{i=2}^{q} c_i \mathbf{v}_i \in \mathsf{K}^r$ avec au moins un $c_i \neq 0$, donc $\mathbf{v}_2, \ldots, \mathbf{v}_q$ sont linéairement dépendants, contradiction avec l'hypothèse. Donc $c_1 = \sum_{i=2}^{q} c_i b_i \neq 0$ et $\mathbf{v_1} = c_1^{-1}(\mathbf{w} - \sum_{i=2}^{q} c_i \mathbf{v}_i)$.

En numérotant si nécessaire, on suppose que $c_2 \neq 0$. Si les $\mathbf{v}'_3, \ldots, \mathbf{v}'_{q+1}$ sont linéairement dépendants, en raisonnant de la même manière on obtient $\mathbf{v_1} = d_1^{-1}(\mathbf{z} - \sum_{i=3}^{q+1} d_i \mathbf{v}_i)$ avec $d_1 \neq 0$.

(3) Alors $d_1\mathbf{w} - c_1\mathbf{z} = d_1 c_2 \mathbf{v}_2 + \sum_{i=3}^{q+1} (d_1 c_i - d_i c_1)\mathbf{v}_i - c_1 d_{q+1} \mathbf{v}_{q+1} \in \mathsf{K}^r$ avec $d_1 c_2 \neq 0$ ce qui contredit l'indépendance de $\mathbf{v}'_2, \ldots, \mathbf{v}'_{q+1}$.

Question 6 : Correction : On procède par récurrence sur le rang colonne modulo K de $\mathbf{A}$. Nous démarrons la récurrence à $q = 1$ afin de nous servir de ce résultat dans l'étape inductive (le cas $q = 0$ est trivial).

Soit $q = 1$: D'après la définition du rang colonne, une colonne de $\mathbf{A}$ a des termes en $\mathsf{K}[a_1, \ldots, a_n]$. Supposons par absurde qu'il n'y a pas de multiplication active. Alors on a jamais $f_i \leftarrow op_i \times op_j$ avec op_i contenant un x_i et $op_j \notin \mathsf{K}$. On déduit que les résultats du calcul s'écrivent $\sum_i c_i x_i + P(a_1, \ldots, a_n)$ où P est un polynôme, et $c_i \in \mathsf{K}$. Les c_i sont nécessairement les coefficients de $\mathbf{A}$, donc $\mathbf{A}$ est une matrice à valeurs dans K et par conséquence son rang colonne modulo K est 0, contradiction. Donc il y a au moins une $(= q)$ multiplication active.

Soit $q > 1$ et supposons la propriété vraie pour $q - 1 > 0$. On sait qu'il y a au moins une multiplication active $(q - 1 > 0)$. Soit $f_i \leftarrow g \times h$ la première multiplication active du calcul avec $g = \sum_i c_i x_i + P(a_1, \ldots, a_n)$ (même raisonnement que pour le cas de base). On suppose sans perte de généralité que $c_1 \neq 0$ (il y a forcement un $c_i \neq 0$ sinon la multiplication n'est pas active).

On fabrique un nouveau calcul à partir du calcul considéré de la manière suivante. On enlève la première composante du vecteur $\mathbf{x}$ des paramètres en la définissant par $x_1 = -c_1^{-1}(\sum_{i=2}^{p} c_i x_i + P(a_1, \ldots, a_n))$. Alors $g = 0$ et donc on peut remplacer $f_i \leftarrow g \times h$ par $f_i \leftarrow 0$. On effectue le calcul $\mathbf{Ax} + \mathbf{y}$ dans ce cas particulier, ce qui s'exprime comme $\mathbf{A'x'} + \mathbf{y'}$ avec $\mathbf{x'} = (x_2, \ldots, x_p)$, $\mathbf{y'} = \mathbf{y} - c_1^{-1} P(a_1, \ldots, a_n)\mathbf{A}[-, 1]$, et pour $i \geq 1$, $\mathbf{A'}[-, i] = \mathbf{A}[-, i+1] - c_1^{-1} c_i \mathbf{A}[-, 1]$. (Intuitivement, on supprime la colonne 1 de $\mathbf{A}$ et on décale les résultats).

Alors l'ensemble des vecteurs colonne de $\mathbf{A'}$ rentrent dans le cadre de la question 5, et le rang colonne modulo K de $\mathbf{A'}$ est au moins égal à $q - 1$, donc le nouveau calcul comporte au moins $q-1$ multiplications actives (par hypothèse de récurrence). Pour effectuer le calcul normal il faut faire $g \times h$ en plus, d'où au moins q multiplications actives.

Question 7 : Correction : Le produit matrice vecteur $\mathbf{Ax}$ avec $\mathbf{A}= (a_{i,j})_{n \times p}$ et $\mathbf{x} = (x_1, \ldots, x_p)$ se réécrit :

$$\begin{bmatrix} x_1 & \cdots & x_p & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \cdot & & & & & & & & \cdot \\ \cdot & & & & & & & & \cdot \\ \cdot & & & & & & & & \cdot \\ 0 & \cdots & 0 & 0 & \cdots & 0 & x_1 & \cdots & x_p \end{bmatrix} \times \begin{bmatrix} a_{1,1} \\ \cdots \\ a_{1,p} \\ \cdots \\ a_{n,1} \\ \cdots \\ a_{n,p} \end{bmatrix}$$

Il est alors immédiat que np vecteurs colonne de cette nouvelle matrice sont linéairement indépendants modulo K, et donc le calcul a au moins np multiplications (question 6).

2 Forme normale algébrique d'une fonction booléenne

Question 8 : Correction : Pour deux variables

$$f(x_1, x_2) = g(0,0) \oplus g(1,0)x_1 \oplus g(0,1)x_2 \oplus g(1,1)x_1x_2$$

On déduit une façon de calculer g en fonction de f :

$$\begin{aligned} f(0,0) &= g(0,0) \\ f(1,0) &= g(0,0) \oplus g(1,0) \\ f(0,1) &= g(0,0) \oplus g(0,1) \\ f(1,1) &= g(0,0) \oplus g(1,0) \oplus g(0,1) \oplus g(1,1) \end{aligned}$$

Cette façon s'étend au cas général, g étant fixé par le tableau de vérité de f.

Question 9 : Correction : Pour $n = 1$ on a $f(x_1) = g(0) \oplus g(1)x_1$ avec $f(0) = g(0)$ et $f(1) = g(0) \oplus g(1)$. D'après le tableau de vérité, $g(1) = f(0) \oplus f(1)$.

Question 10 : Correction : D'après la forme polynomiale de f, $f(x_1, \ldots, x_n) = \underbrace{\sum_{(a_1,\ldots,a_{n-1},0)\in\mathbb{B}^n} g(a_1, \ldots, a_{n-1}, 0) \cdot x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}}_{f_0(x_1,\ldots,x_{n-1})} + x_n \underbrace{\sum_{(a_1,\ldots,a_{n-1},1)\in\mathbb{B}^n} g(a_1, \ldots, a_{n-1}, 1) \cdot x_1^{a_1} \cdots x_{n-1}^{a_{n-1}}}_{f_1(x_1,\ldots,x_{n-1})}$

Question 11 : <u>Correction</u> : On a

$$\begin{aligned}
f_0(x_1,\dots,x_{n-1}) &= \sum_{(a_1,\dots,a_{n-1})\in\mathbb{B}^{n-1}} g_0(a_1,\dots,a_{n-1}).x_1^{a_1}\cdots x_{n-1}^{a_{n-1}} \\
f_1(x_1,\dots,x_{n-1}) &= \sum_{(a_1,\dots,a_{n-1})\in\mathbb{B}^{n-1}} g_1(a_1,\dots,a_{n-1}).x_1^{a_1}\cdots x_{n-1}^{a_{n-1}} \\
f(x_1,\dots,x_n) &= \sum_{(a_1,\dots,a_{n-1})\in\mathbb{B}^{n-1}} g_0(a_1,\dots,a_{n-1}).x_1^{a_1}\cdots x_{n-1}^{a_{n-1}} \\
&\quad + \sum_{(a_1,\dots,a_{n-1})\in\mathbb{B}^{n-1}} g_1(a_1,\dots,a_{n-1}).x_1^{a_1}\cdots x_{n-1}^{a_{n-1}}x_n
\end{aligned}$$

Donc

$$\begin{aligned}
g(x_1,\dots,x_{n-1},0) &= g_0(x_1,\dots,x_{n-1}) \\
g(x_1,\dots,x_{n-1},1) &= g_1(x_1,\dots,x_{n-1})
\end{aligned}$$