TD 5 – Bornes inférieures de complexité en calcul formel

Margot Catinaud margot.catinaud@lmf.cnrs.fr
Valentin Dardilhac valentin.dardilhac87@gmail.com

I Bornes inférieures de complexité en calcul arithmétique

Définition 1 : Calcul arithmétique

Un *calcul arithmétique* sur un corps $\mathbb{K}$ à partir d'un ensemble de paramètres $\pi \overset{\text{def}}{=} \{\pi_i\}_{i=1}^n \in \mathbb{K}^n$ est une suite d'instructions du type :

$$\left(x_i \leftarrow o_i \ \mathsf{op}_i \ o_i';\right)_{i=1}^k$$

avec, pour tout $i \in [\![1;k]\!]$,

- x_i une *variable de calcul* ;
- $\mathsf{op}_i \in \{+,-,\times\}$ une *opération* ;
- o_i, o_i' des *opérandes* pouvant être soit (i) des éléments du corps $\mathbb{K}$, soit (ii) des paramètres de π ; soit (iii) l'une des variables de $\{x_i\}_{i=1}^{k-1}$.

Par exemple, le programme ci-dessous calcule le produit de deux nombres complexes $(a+ib)(c+id)$; le résultat étant $x_3 + ix_6$ et les paramètres sont $\pi = \{a,b,c,d\} \subset \mathbb{R}$:

$$\begin{array}{lll} x_1 \leftarrow a \times c; & x_3 \leftarrow x_1 - x_2; & x_5 \leftarrow b \times c; \\ x_2 \leftarrow b \times d; & x_4 \leftarrow a \times d; & x_6 \leftarrow x_4 + x_5; \end{array}$$

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

Question 2 *Soit un calcul arithmétique qui renvoie $r \in \mathbb{N}$ résultats et qui comprend $s \in \mathbb{N}$ multiplications. Montrer que le vecteur des résultats, noté $\mathbf{v}$, vérifie $\mathbf{v} = \mathbf{M} \cdot \mathbf{e} + \mathbf{h}$ avec*

- $\mathbf{M} \in \mathcal{M}_{r\times s}(\mathbb{K})$ *est une matrice à valeurs dans $\mathbb{K}$ de r lignes et s colonnes ;*
- $\mathbf{e}$ *est un vecteur de dimension s à valeurs dans $\mathbb{K}[\pi_1,\dots,\pi_n]$ (l'anneau des polynômes multivariés, dont les variables sont les paramètres $\pi = \{\pi_i\}_{i=1}^n$) ;*
- *et $\mathbf{h} \in \mathbb{K}^r$ est un vecteur de dimension r dont les coefficients sont de la forme :*

$$\forall\, i \in [\![1;r]\!],\ h_i \overset{def}{=} c_0 + \sum_{j=1}^{n} c_j \pi_j \qquad \text{avec } c_i \in \mathbb{K}.$$

Définition 2 : Vecteurs linéairement indépendants modulo un corps, rang

Soient $\mathbf{v}_1,\dots,\mathbf{v}_m$ $m \in \mathbb{N}$ vecteurs de dimension r à coefficients dans l'anneau $\mathbb{K}[\pi_1,\dots,\pi_n]$. On dit que la famille de vecteurs $\mathcal{V} \overset{\text{def}}{=} (\mathbf{v}_i)_{i=1}^m$ est *une famille de vecteurs linéairement indépendants modulo le corps* $\mathbb{K}$ lorsque :

$$\forall\, \lambda_1,\dots,\lambda_m \in \mathbb{K},\ \left[\sum_{i=1}^{m} \lambda_i \mathbf{v}_i \in \mathbb{K}^r \implies \forall\, i \in [\![1;m]\!],\ \lambda_i = 0\right].$$

On appelle *rang ligne (resp. colonne) modulo le corps* $\mathbb{K}$ d'une matrice $\mathbf{M}$ à coefficients dans l'anneau $\mathbb{K}[\pi_1,\dots,\pi_n]$ le nombre maximal de vecteurs ligne (resp. colonne) de $\mathbf{M}$ linéairement indépendants modulo $\mathbb{K}$.

Question 3 Considérons un calcul arithmétique Γ qui effectue le produit matrice-vecteur $\mathbf{Mx}$ avec $\mathbf{M}$ une matrice de dimension $r \times p$ à coefficients dans l'anneau $\mathbb{K}\big[\pi_1, \ldots, \pi_n\big]$ et $\mathbf{x} = (x_i)_{i=1}^p \in \mathbb{K}^p$ un vecteur. Les paramètres de ce calcul sont $\pi_\Gamma = \{\pi_i\}_{i=1}^n \cup \{x_i\}_{i=1}^p$. On souhaite montrer que le nombre de multiplications de ce calcul est au moins r pour le pire des cas (lorsqu'il n'y a pas de coefficients nuls dans $\mathbf{M}$). Pour cela, on suppose par l'absurde que le rang ligne modulo $\mathbb{K}$ de $\mathbf{M}$ vaut r et que $r > s$, où s est le nombre de multiplications du calcul Γ.

1. *Montrer qu'il existe un vecteur $\mathbf{y} \in \mathbb{K}^r$ à coefficients dans $\mathbb{K}$ non nul et un vecteur $\mathbf{h} \in \mathbb{K}^p$ à coefficients de la forme*
$$\forall\, i \in [\![1; p]\!],\ h_i \overset{def}{=} \underbrace{c_0}_{\in\mathbb{K}} + \sum_{j=1}^{n} \underbrace{c_j}_{\in\mathbb{K}} \pi_j + \sum_{j=1}^{p} \underbrace{c'_j}_{\in\mathbb{K}} x_j$$
vérifiant l'égalité $\mathbf{y}^T\mathbf{Mx} = \mathbf{y}^T\mathbf{h}$.
2. *Montrer que $\mathbf{y}^T\mathbf{M}$ est un vecteur ligne à valeurs dans $\mathbb{K}$.*
3. *Conclure.*

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

Question 5 Soit $\mathcal{V} = \{\mathbf{v}_i\}_{i=1}^m$ un ensemble de vecteurs de dimension r à coefficients dans l'anneau $\mathbb{K}\big[\pi_1, \ldots, \pi_n\big]$ contenant q vecteurs linéairement indépendants modulo $\mathbb{K}$. On considère, pour $i \in [\![2; n]\!]$, $\mathbf{v}'_i \overset{\text{def}}{=} \mathbf{v}_i + b_i\mathbf{v}_1$ avec $b_i \in \mathbb{K}$. On souhaite montrer qu'il existe $q-1$ vecteurs $\mathbf{v}'_i$ linéairement indépendants modulo $\mathbb{K}$.

1. *Établir le résultat lorsque $\{\mathbf{v}_i\}_{i=1}^q$ sont linéairements indépendants modulo $\mathbb{K}$.*

On suppose désormais (quitte à réordonner) que $\{\mathbf{v}_i\}_{i=2}^{q+1}$ sont linéairement indépendants modulo $\mathbb{K}$, *i.e.* le vecteur $\mathbf{v}_1$ n'est pas dans les $q-1$ vecteurs linéairement indépendants.

2. *Par l'absurde, supposons que les deux ensembles $\{\mathbf{v}'_i\}_{i=2}^q$ et $\{\mathbf{v}'_i\}_{i=3}^{q+1}$ sont des ensembles de vecteurs linéairement dépendants modulo $\mathbb{K}$. Montrer qu'il existe des coefficients $\lambda_1, \ldots, \lambda_q \in \mathbb{K}$ tels que $\sum_{i=1}^{q} \lambda_i\mathbf{v}_i = \mathbf{w} \in \mathbb{K}^r$, $\lambda_1 \neq 0$ et $(\lambda_i)_{i=2}^q$ non tous nuls. On suppose dans la suite, quitte à réordonner, que $\lambda_2 \neq 0$.*
3. *En déduire de même qu'il existe $\mathbf{z} \in \mathbb{K}^r$, $\mu_1 \neq 0$ et $(\mu_i)_{i=3}^{q+1}$ des coefficients de $\mathbb{K}$ non tous nuls vérifiant*
$$\mu_1\mathbf{v}_1 + \sum_{i=3}^{q+1} \mu_i\mathbf{v}_i = \mathbf{z}.$$
4. *Exprimer $\mu_1\mathbf{w} - \lambda_1\mathbf{z}$ à l'aide des coefficients λ_i et μ_i afin d'obtenir une contradiction.*

Soit le calcul arithmétique qui effectue le produit matrice-vecteur $\mathbf{Mx}+\mathbf{y}$ où $\mathbf{M}$ est une matrice de dimension $r \times p$ à coefficients dans l'anneau $\mathbb{K}\big[\pi_1, \ldots, \pi_n\big]$, $\mathbf{x} = (x_i)_{i=1}^p \in \mathbb{K}^p$ et $\mathbf{y} = (y_i)_{i=1}^r$ un vecteur de dimension r à valeurs dans $\mathbb{K}\big[\pi_1, \ldots, \pi_n\big]$. Les paramètres de ce calcul sont $\pi = \{\pi_i\}_{i=1}^n \cup \{x_i\}_{i=1}^p$. Une multiplication de ce calcul est qualifiée d'*active* lorsque l'une des opérandes 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 $\mathbf{M}$. On pourra procéder par récurrence sur le rang colonne.*

Question 7 *En déduire qu'un calcul du produit d'une matrice de dimension $n \times p$ par un vecteur de dimension p où les paramètres sont les coefficients de la matrice et du vecteur requiert* au moins *np multiplications.*

II Forme normale algébrique d'une fonction booléenne

Question 8 (Question préliminaire) *On note* $\mathbb{B} = \{0, 1\}$. *Rappeler et montrer pour quelles opérations* $\mathbb{B}$ *est un corps.*

Dans la suite, on note $\oplus$ et $\odot$ les opérations précisées dans la question précédente. On s'intéresse à une fonction booléenne $f : \mathbb{B}^n \longrightarrow \mathbb{B}$. Cette fonction peut être représentée par sa table de vérité ou, plus couramment, comme un polynôme à plusieurs variables de degré au plus n sur l'anneau $\mathbb{B}\big[x_1, \ldots, x_n\big]$.

Question 9 (Forme Normale Algébrique (ANF)) *Montrer que* f *peut s'écrire sous la forme*

$$f(x_1, \ldots, x_n) = \bigoplus_{(b_1,\ldots,b_n)\in\mathbb{B}^n} \left(g(b_1, \ldots, b_n) \cdot \bigodot_{i=1}^{n} (x_i)^{b_i} \right),$$

où $g : \mathbb{B}^n \longrightarrow \mathbb{B}$.

La représentation de la question précédente est appelée la *Forme Normale Algébrique (ou Algebraic Normale Form (ANF))* de la fonction f.[1]

Question 10 *Exprimer* g *dans le cas où* $n = 1$.

Question 11 *Montrer que la procédure qui calcule* g *en fonction de* f *est* involutive, *c'est-à-dire qu'elle permet également de calculer* f *en fonction de* g.

Question 12 *Montrer que* f *peut s'écrire sous la forme*

$$f(x_1, \ldots, x_n) = f_0(x_1, \ldots, x_{n-1}) \oplus \big(x_n \odot f_1(x_1, \ldots, x_{n-1})\big)$$

pour deux fonctions f_0 *et* f_1 *que l'on précisera.*

Question 13 *Soit* g_0 *et* g_1 *les ANF de* f_0 *et respectivement* f_1. *Exprimer* g *en fonction de* g_0 *et* g_1.

Devoir maison 5 *En déduire un algorithme de calcul de* g *et donner sa complexité.*

1. Pour aller plus loin au sujet des fonctions booléenne et des ANF, voir par exemple
   - https://youtu.be/iYw3sOojd2M – cours de Anne Canteaut, Directrice de Recherche INRIA, cryptographe symmétricienne ;
   - https://hal.science/tel-05020635 – thèse de Jules Baudrin, Maitre de Conférence à l'UVSQ, cryptographe symmétricien ;
   - ...