Soutenance de stage au LIRMM

Résolution efficace de systèmes linéaires à coefficients polynomiaux

Dorian Lesbre
Encadrants: Romain Lebreton et Pascal Giorgi

2 septembre 2019

1. Introduction

2. Étude du high-order lifting
   - Suites récurrentes
   - Sous-problèmes
   - High-order lifting
   - Second-membre non borné

3. Résultats expérimentaux
   - Travail d'implémentation
   - Résultats

Introduction

Problème

Résolution modulaire de système linéaire

Soit C une matrice $n \times n$ sur $\mathbb{K}[X]$, notons d son degré.

Soit N un vecteur $n \times 1$ sur $\mathbb{K}[X]$.

Soit $k \in \mathbb{N}$, nous cherchons un vecteur U tel que :

$$CU \equiv N \mod X^{d2^k}$$

Méthodes de résolution

Algorithmes connus :

- Pivot de Gauss en $O(MM(n)M(d2^k))$
- 1979, Mœnck et Carter en $O(n^2M(d)2^k)$
- 1982, Dixon, version alternative de même complexité
- 2002, Storjohann en $O(MM(n)M(d)k)$

Pour pouvoir résoudre exactement par reconstruction rationnelle, il faut $2^k \geqslant n$

Étude du high-order lifting

Suite récurrente de matrice

Définition

Soit (C_i) $d+1$ matrices carrées non toutes nulles, une suite récurrente de matrice (U_i) vérifie :

$$\forall \ell \in \mathbb{N}, \sum_{i=0}^{d} C_i U_{i+\ell} = 0_{n \times m}$$

Exemple : $U_i = \begin{bmatrix} a_i \\ b_i \end{bmatrix}$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_{n+2} \\ b_{n+2} \end{bmatrix} + \begin{bmatrix} -1 & 3 \\ 15 & 7 \end{bmatrix} \begin{bmatrix} a_{n+1} \\ b_{n+1} \end{bmatrix} + \begin{bmatrix} 7 & 3 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a_n \\ b_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}$$

Rationalité de U

Notation sous forme de série formelle :

$$U = \sum_{k=0}^{+\infty} U_k X^k \quad \text{et} \quad C = \sum_{k=0}^{d} C_{d-k} X^k$$

Théorème

Il existe $N \in \mathbb{K}[X]^n$ de degré strictement inférieur à d telle que

$$CU = N$$

Trois représentations

Trois représentations : une suite récurrente peut être représentée par,

- l'ensemble de ses termes $(U_i)_{i\in\mathbb{N}}$
- les termes initiaux $(U_0, \ldots, U_d)$ et C.
- le numérateur N de degré inférieur à d et C.

Sous-problèmes

Calcul des termes suivants

Étant donné C inversible modulo X^d et les premiers termes $(U_0, \ldots, U_{d-1})$, nous voulons calculer les termes suivants de la suite (U_i).

Résolution de système borné

Étant donné C inversible modulo X^d, N et $k \in \mathbb{N}$, avec $\deg N, \deg C < d$, nous cherchons $U \in \mathbb{K}[X]^n$ tel que

$$CU \equiv N \mod X^{d2^k}$$

Regroupement X^d-adique

Pour simplifier les calculs, nous passerons en X^d-adique dans la suite. Nous noterons $\widehat{U}_i$ les coefficients X^d-adiques de U :

$$U = \sum_{k=0}^{+\infty} \widehat{U}_k X^{kd}$$

Avec $\deg \widehat{U}_i < d$.

Produit : $\widehat{A} \times \widehat{B}$ a un degré borné par $2d$. Posons,

- $\underline{\widehat{A}\widehat{B}}$ la partie haute (quotient par X^d)
- $\overline{\widehat{A}\widehat{B}}$ la partie basse (reste)

Suite décalée

Définition

Si $(U_i)_{i\in\mathbb{N}}$ est une suite récurrente de générateur C, alors pour tout $\ell \in \mathbb{N}$, $(U_i)_{i\geqslant\ell}$ est aussi une suite récurrente de même générateur C, nous parlons de *suite décalée* de ℓ.

Théorème

Pour $i \in \mathbb{N}$, posons $N_i = \overline{C\widehat{U_i}}$ le numérateur correspondant à la suite décalée de *id*. Cette suite de numérateurs vérifie :

$$\forall i \in \mathbb{N}, N_{i+1} \equiv -\underline{C\widehat{U_i}} \mod X^d$$

Cette relation effectue un changement de représentation.

High-order lifting

Théorème

En notant $D = \sum \widehat{D}_i X^{id}$ l'inverse de C nous avons :

$$\forall j \in \mathbb{N}, \forall \ell \in \mathbb{N},\ \widehat{U}_{\ell+j} = \underline{\widehat{D}_{j-1} N_\ell} + \overline{\widehat{D}_j N_\ell}$$

avec $\widehat{D}_{-1} = 0$

Preuve : par rationalité de $(U_{i+\ell})$, $U = DN$. En identifiant les coefficients nous obtenons la relation ci-dessus.

Résolution 1/2 : composantes de l'inverse

Nous pouvons faire un pas de j sur toute suite récurrente en connaissant $\widehat{D}_{j-1}$ et $\widehat{D}_j$.

Or $CD = I$, donc (D_i) est une suite récurrente. Nous pouvons lui appliquer le théorème :

$\widehat{D}_0$ $\widehat{D}_1$ $\widehat{D}_2$ $\widehat{D}_3$ $\widehat{D}_4$ $\widehat{D}_5$ $\widehat{D}_6$ $\widehat{D}_7$ $\widehat{D}_8$ $\widehat{D}_9$ $\widehat{D}_{10}$ $\widehat{D}_{11}$ $\widehat{D}_{12}$ $\widehat{D}_{13}$ $\widehat{D}_{14}$ $\widehat{D}_{15}$

$\widehat{D}_0$ $\widehat{D}_1$ $\widehat{D}_2$ $\widehat{D}_3$ $\widehat{D}_4$ $\widehat{D}_5$ $\widehat{D}_6$ $\widehat{D}_7$ $\widehat{D}_8$ $\widehat{D}_9$ $\widehat{D}_{10}$ $\widehat{D}_{11}$ $\widehat{D}_{12}$ $\widehat{D}_{13}$ $\widehat{D}_{14}$ $\widehat{D}_{15}$

$\widehat{D}_0$ $\widehat{D}_1$ $\widehat{D}_2$ $\widehat{D}_3$ $\widehat{D}_4$ $\widehat{D}_5$ $\widehat{D}_6$ $\widehat{D}_7$ $\widehat{D}_8$ $\widehat{D}_9$ $\widehat{D}_{10}$ $\widehat{D}_{11}$ $\widehat{D}_{12}$ $\widehat{D}_{13}$ $\widehat{D}_{14}$ $\widehat{D}_{15}$

$\widehat{D}_0$ $\widehat{D}_1$ $\widehat{D}_2$ $\widehat{D}_3$ $\widehat{D}_4$ $\widehat{D}_5$ $\widehat{D}_6$ $\widehat{D}_7$ $\widehat{D}_8$ $\widehat{D}_9$ $\widehat{D}_{10}$ $\widehat{D}_{11}$ $\widehat{D}_{12}$ $\widehat{D}_{13}$ $\widehat{D}_{14}$ $\widehat{D}_{15}$

Résolution (2/2) : composantes de la solution

Avec les $\widehat{D}_{2^j-1}$ et $\widehat{D}_{2^j}$, nous pouvons faire des pas de 2^j pour calculer la solution :

$$\widehat{U}_0 \; \widehat{U}_1 \; \widehat{U}_2 \; \widehat{U}_3 \; \widehat{U}_4 \; \widehat{U}_5 \; \widehat{U}_6 \; \widehat{U}_7 \; \widehat{U}_8 \; \widehat{U}_9 \; \widehat{U}_{10} \; \widehat{U}_{11} \; \widehat{U}_{12} \; \widehat{U}_{13} \; \widehat{U}_{14} \; \widehat{U}_{15}$$

$$\widehat{U}_0 \; \widehat{U}_1 \; \widehat{U}_2 \; \widehat{U}_3 \; \widehat{U}_4 \; \widehat{U}_5 \; \widehat{U}_6 \; \widehat{U}_7 \; \widehat{U}_8 \; \widehat{U}_9 \; \widehat{U}_{10} \; \widehat{U}_{11} \; \widehat{U}_{12} \; \widehat{U}_{13} \; \widehat{U}_{14} \; \widehat{U}_{15}$$

$$\widehat{U}_0 \; \widehat{U}_1 \; \widehat{U}_2 \; \widehat{U}_3 \; \widehat{U}_4 \; \widehat{U}_5 \; \widehat{U}_6 \; \widehat{U}_7 \; \widehat{U}_8 \; \widehat{U}_9 \; \widehat{U}_{10} \; \widehat{U}_{11} \; \widehat{U}_{12} \; \widehat{U}_{13} \; \widehat{U}_{14} \; \widehat{U}_{15}$$

$$\widehat{U}_0 \; \widehat{U}_1 \; \widehat{U}_2 \; \widehat{U}_3 \; \widehat{U}_4 \; \widehat{U}_5 \; \widehat{U}_6 \; \widehat{U}_7 \; \widehat{U}_8 \; \widehat{U}_9 \; \widehat{U}_{10} \; \widehat{U}_{11} \; \widehat{U}_{12} \; \widehat{U}_{13} \; \widehat{U}_{14} \; \widehat{U}_{15}$$

$$\widehat{U}_0 \; \widehat{U}_1 \; \widehat{U}_2 \; \widehat{U}_3 \; \widehat{U}_4 \; \widehat{U}_5 \; \widehat{U}_6 \; \widehat{U}_7 \; \widehat{U}_8 \; \widehat{U}_9 \; \widehat{U}_{10} \; \widehat{U}_{11} \; \widehat{U}_{12} \; \widehat{U}_{13} \; \widehat{U}_{14} \; \widehat{U}_{15}$$

Second membre non borné

Résolution de système

Soit $C \in \mathcal{M}_n(\mathbb{K}[X])$ inversible modulo X^d, $k \in \mathbb{N}$, et $N = \sum_{i=0}^{2^k-1} \widehat{N}_i X^{id}$. Nous supposons toujours $\deg C < d$, nous cherchons U tel que

$$CU \equiv N \mod X^{d2^k}$$

Travail sur les numérateurs

Soit $(V^{(j)})$ la suite solution de $CV^{(j)} = \widehat{N}_j$. La solution est

$$U = \sum V^{(j)} X^{dj}$$

Soit $\widehat{N}_{j,\ell}$ les numérateurs de la suite décalée $(\widehat{V}^{(j)}_{p+d\ell})_{p\geqslant 0}$. Alors pour tout p :

$$\widehat{U}_p = \overline{\widehat{D}_0 \sum_{j=0}^{p} \widehat{N}_{j,p-j}}$$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Calcul des numérateurs

Nous pouvons les représenter sous forme d'un tableau :

U	$\widehat{U}_0$	$\widehat{U}_1$	$\widehat{U}_2$	$\widehat{U}_3$	$\widehat{U}_4$	$\widehat{U}_5$	$\widehat{U}_6$	$\widehat{U}_7$
$V^{(0)}$	$\widehat{N}_{0,0}$	$\widehat{N}_{0,1}$	$\widehat{N}_{0,2}$	$\widehat{N}_{0,3}$	$\widehat{N}_{0,4}$	$\widehat{N}_{0,5}$	$\widehat{N}_{0,6}$	$\widehat{N}_{0,7}$
$V^{(1)}$		$\widehat{N}_{1,0}$	$\widehat{N}_{1,1}$	$\widehat{N}_{1,2}$	$\widehat{N}_{1,3}$	$\widehat{N}_{1,4}$	$\widehat{N}_{1,5}$	$\widehat{N}_{1,6}$
$V^{(2)}$			$\widehat{N}_{2,0}$	$\widehat{N}_{2,1}$	$\widehat{N}_{2,2}$	$\widehat{N}_{2,3}$	$\widehat{N}_{2,4}$	$\widehat{N}_{2,5}$
$V^{(3)}$				$\widehat{N}_{3,0}$	$\widehat{N}_{3,1}$	$\widehat{N}_{3,2}$	$\widehat{N}_{3,3}$	$\widehat{N}_{3,4}$
$V^{(4)}$					$\widehat{N}_{4,0}$	$\widehat{N}_{4,1}$	$\widehat{N}_{4,2}$	$\widehat{N}_{4,3}$
$V^{(5)}$						$\widehat{N}_{5,0}$	$\widehat{N}_{5,1}$	$\widehat{N}_{5,2}$
$V^{(6)}$							$\widehat{N}_{6,0}$	$\widehat{N}_{6,1}$
$V^{(7)}$								$\widehat{N}_{7,0}$

Résultats expérimentaux

Partie expérimentale

Implémentation en SageMath :

- évaluation et interpolation pour le produits de polynômes et matrices polynomiales
- Résolution de systèmes modulaires polynomiaux :
  - méthode de Dixon
  - méthode de Mœnck et Carter
  - méthode de Storjohann
  - notre méthode de high-order lifting
- ajout de produits matriciels polynomiaux dans SageMath depuis Linbox

Test de correction et comparaisons des temps d'exécution

Regroupement de produits matrice-vecteur

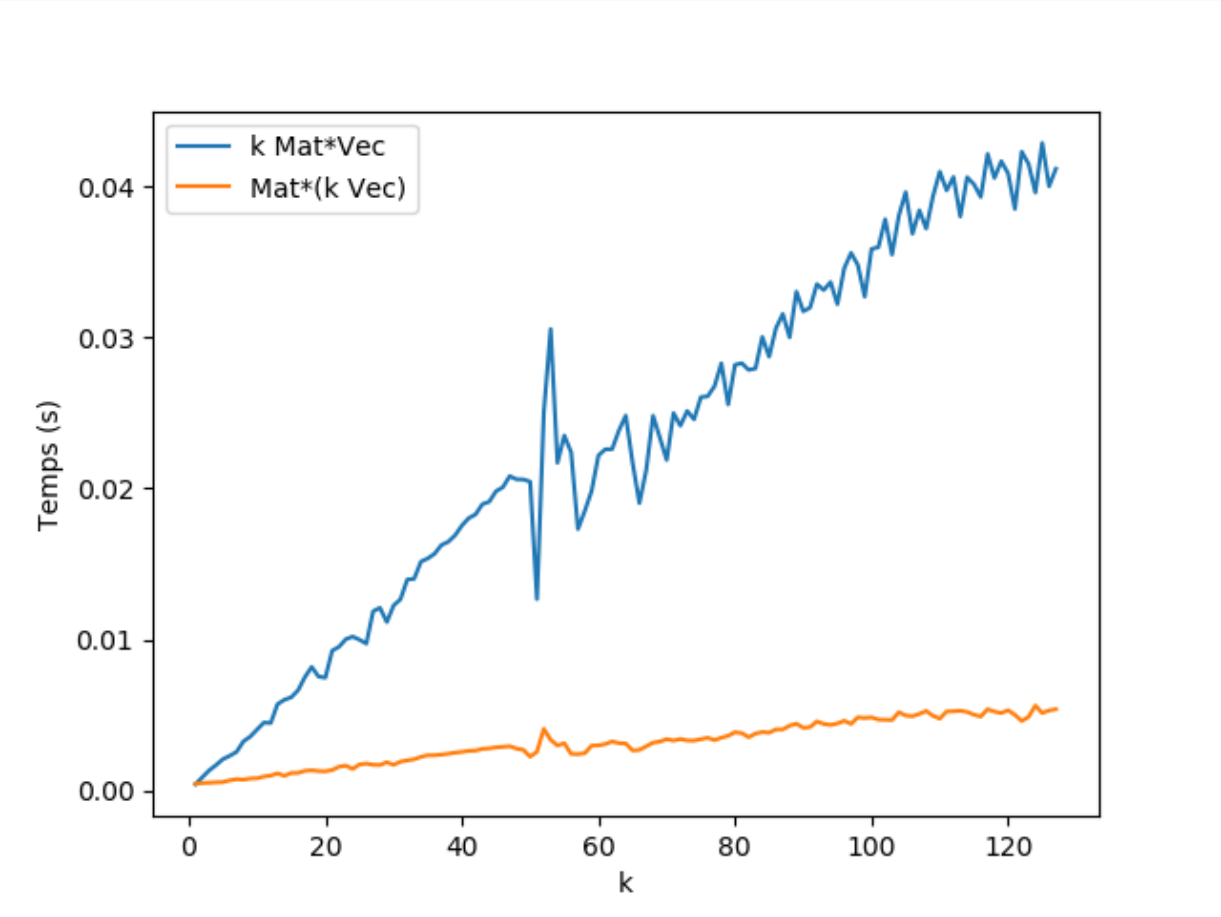

Figure 1 – Temps d'exécution de k produit matrices $(n \times n)$ vecteurs $(n \times 1)$ et d'un produit matrice $(n \times n)$ matrice $(n \times k)$ pour $n = 128$ dans le corps premier $\mathbb{F}_{524309}$

Complexité d'évaluation interpolation

Pour un produit matrice-vecteur à coefficient polynomiaux, nous avons les complexité suivantes :

- produit naïf en $O(n^2 M(d))$
- évaluation interpolation en $O(n^2 M(d) + n^2 d + nM(d))$
- évaluation précalculée en $O(nM(d) + n^2 d + nM(d))$

Temps d'évaluation interpolation

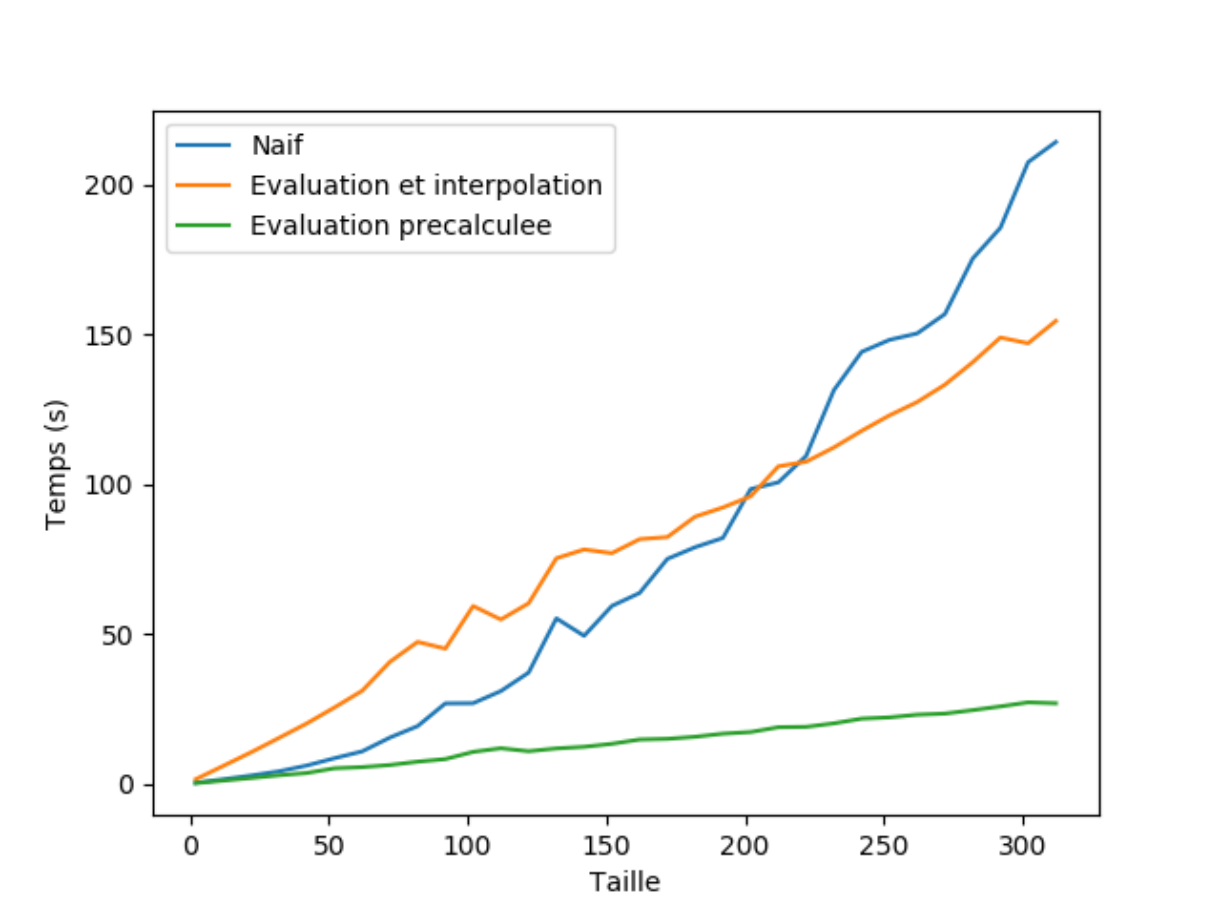

Figure 2 – Temps d'exécution de différents produits de matrices polynomiales sur $\mathbb{F}_{524309}$ de degré $d = 128$ en fonction de la taille des matrices

Complexité de résolution de système

Les résolutions vues ont les complexité suivante pour résoudre jusqu'à l'ordre n :

- résolution de système dans l'anneau quotient : $O(MM(n)M(nd))$
- méthode de Dixon ou Mœnck et Carter : $O(n^2 M(d)n)$
- high-order lifting : $O(MM(n)M(d)\log n)$

Résolution de système par degré

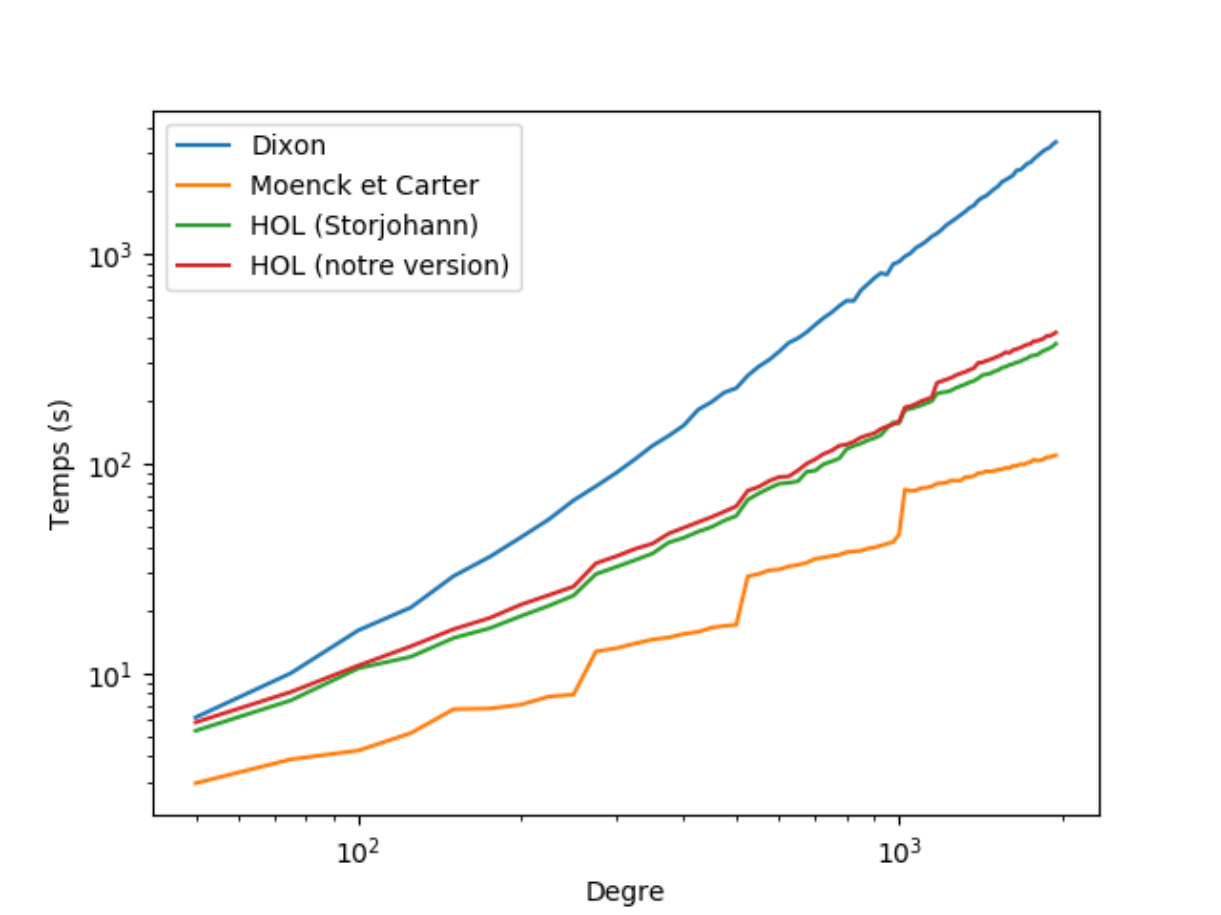

Figure 3 – Temps d'exécution des résolutions pour des systèmes de taille $n = 32$ jusqu'à l'ordre $32d$ en fonction du degré d (échelle logarithmique) sur $\mathbb{F}_{524309}$

Résolution de système par taille

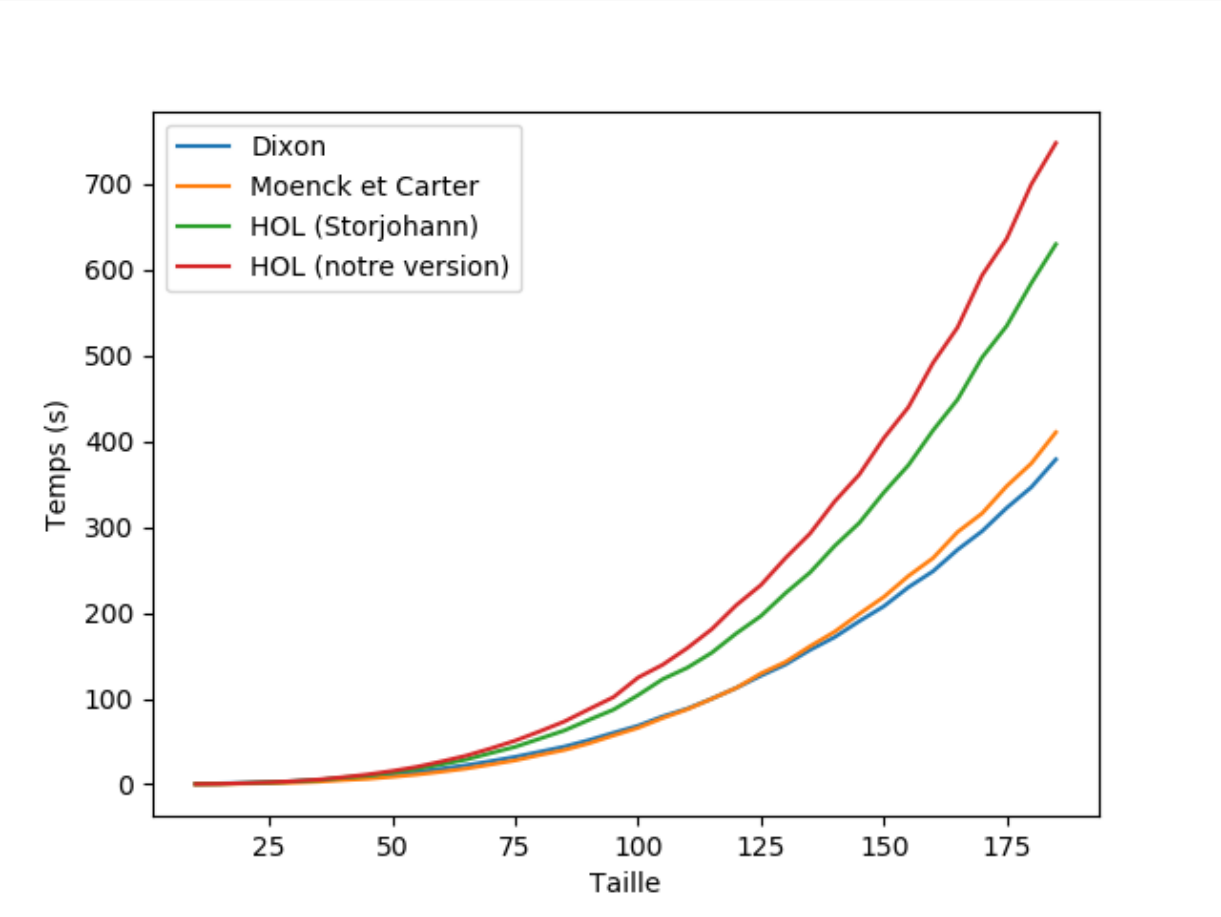

Figure 4 – Temps d'exécution des résolutions pour des systèmes de matrices polynomiales de degré $d = 32$ jusqu'à l'ordre $1024 = 32d$ en fonction de leur taille n sur $\mathbb{F}_{524309}$

Remerciements

Je tenais à remercier mes encadrants, Romain Lebreton et Pascal Giorgi pour m'avoir accueilli et aidé tout au long du stage, ainsi que toute l'équipe ECO du LIRMM pour son accueil.

Enfin je voudrais remercier Jérémy Berthomieu qui m'a encadré pour mon préstage à Paris.