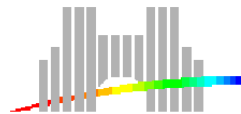


# Calcul du rang et d'une "petite" base du noyau d'une matrice polynomiale

**Gilles Villard**

CNRS, Laboratoire LIP ENS Lyon

Travail réalisé avec Arne Storjohann, U. Waterloo, Ontario, Canada  
Séminaire du projet Algorithmes, INRIA Rocquencourt, 14 mars 2004



# **Introduction et contexte**

## Le problème

$M \in \mathbb{K}[x]^{m \times n}$  **matrice polynomiale** d'une variable,  
calculer son **rang**  $r$ ,  
et son **noyau**, i.e. une matrice  $N \in \mathbb{K}(x)^{(m-r) \times m}$  telle que

$$N \cdot M = 0$$

## Le problème

$M \in \mathbb{K}[x]^{m \times n}$  **matrice polynomiale** d'une variable,  
calculer son **rang**  $r$ ,  
et son **noyau**, i.e. une matrice  $N \in \mathbb{K}(x)^{(m-r) \times m}$  telle que

$$N \cdot M = 0$$

$$\begin{bmatrix} 10 + 9x & 12 + 2x \\ 13 + 14x & 7 + 2x \\ 7 + 13x & 5 + 7x \\ 5 + x & 11 + 10x \end{bmatrix}$$

## Le problème

$M \in \mathbb{K}[x]^{m \times n}$  **matrice polynomiale** d'une variable,  
calculer son **rang**  $r$ ,  
et son **noyau**, i.e. une matrice  $N \in \mathbb{K}(x)^{(m-r) \times m}$  telle que

$$N \cdot M = 0$$

$$\begin{bmatrix} \frac{3x^2+8x+12}{12+6x+x^2} & \frac{2x^2+3x}{12+6x+x^2} & 1 & 0 \\ \frac{10x^2+9x+13}{12+6x+x^2} & \frac{2x^2+16x+5}{12+6x+x^2} & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 10+9x & 12+2x \\ 13+14x & 7+2x \\ 7+13x & 5+7x \\ 5+x & 11+10x \end{bmatrix} = 0 \pmod{17}$$

# Coût cible

## Modèle algébrique sur $K$ [Bürgisser *et al.* 97]

Produit de matrices  
 $\mathbf{A} \cdot \mathbf{B} \ (n \times n)$

$$O(\mathbf{n}^\omega)$$

Déterminant, inversion, polynôme caractéristique,  
**rang, noyau ...**

$$O^{\sim}(\mathbf{n}^\omega)$$

## Coût cible

Modèle algébrique sur  $K$  [Bürgisser *et al.* 97]

Produit de matrices  
 $\mathbf{A} \cdot \mathbf{B}$  ( $n \times n$ )

$$O(\mathbf{n}^\omega)$$

Déterminant, inversion, polynôme caractéristique,  
**rang, noyau ...**

$$O^\sim(\mathbf{n}^\omega)$$

---

Sur  $K[x]$

Produit de matrices  
 $\mathbf{A}(\mathbf{x}) \cdot \mathbf{B}(\mathbf{x})$  ( $n \times n$ , degré  $d$ )

$$\mathbf{MM}(\mathbf{n}, \mathbf{d}) = O^\sim(\mathbf{n}^\omega \mathbf{d})$$

?

$$O^\sim(\mathbf{MM}(\mathbf{n}, \mathbf{d}))$$

## Réductions au produit polynomial matriciel, $O^{\sim}(\text{MM}(n, d))$

- ⊙ **Déterminant**, forme normale de Smith [Storjohann (2002)2003]
- ⊙ **Inversion** générique ( $+n^3d$ ) [JV (2002)2005]
- ⊙ **Puissances itérées** génériques ( $+n^3d$ ),  $A, A^2, \dots, A^n$  [JV 2004]
- ⊙ **Réduction de bases** de modules [GJV 2003]
- ⊙ **Approximation de Padé** à l'ordre  $d$  [BL 1994, GJV 2003]



# Plan de l'exposé

Introduction et contexte

I - Résultats antérieurs

II - Principes de mise en œuvre

III - Bases minimales compressées

IV - L'algorithme

Conclusion

# Plan de l'exposé

Introduction et contexte

**I - Résultats antérieurs**

II - Principes de mise en œuvre

III - Bases minimales compressées

IV - L'algorithme

Conclusion

- ▷ Les **méthodes classiques** (élimination de Gauss) conduisent à des tailles de bases du noyau en  $\Theta(\mathbf{n}^3 \mathbf{d})$  : dans le cas  $2n \times n$ ,  $n$  vecteurs de degré  $nd$
- ~> **Coût**  $n$  fois trop grand, i.e. en  $O^\sim(n^{\omega+1}d)$
  - ~> **Taille en sortie** plus grande que notre coût cible

- ▷ Les **méthodes classiques** (élimination de Gauss) conduisent à des tailles de bases du noyau en  $\Theta(n^3 d)$  : dans le cas  $2n \times n$ ,  $n$  vecteurs de degré  $nd$ 
  - ↪ **Coût**  $n$  fois trop grand, i.e. en  $O^\sim(n^{\omega+1}d)$
  - ↪ **Taille en sortie** plus grande que notre coût cible
  
- ▷ **Algorithme Monte Carlo** pour le rang en  $O^\sim(n^\omega + n^2 d)$ 
  - ↪ **Certification** ? Via le noyau ?

▷ Les **méthodes classiques** (élimination de Gauss) conduisent à des tailles de bases du noyau en  $\Theta(n^3 d)$  : dans le cas  $2n \times n$ ,  $n$  vecteurs de degré  $nd$

↪ **Coût**  $n$  fois trop grand, i.e. en  $O^\sim(n^{\omega+1}d)$

↪ **Taille en sortie** plus grande que notre coût cible

▷ **Algorithme Monte Carlo** pour le rang en  $O^\sim(n^\omega + n^2 d)$

↪ **Certification** ? Via le noyau ?

▷ **Linéarisations** pour le noyau de  $O(n^3 d^2)$  à  $O^\sim(n^{\omega+1}d)$

(“À la main”, faisceaux, résultants & matrices structurées, réalisations ...)

↪ Réduction au **produit de matrice** ?

# Plan de l'exposé

Introduction et contexte

I - Résultats antérieurs

**II - Principes de mise en œuvre**

III - Bases minimales compressées

IV - L'algorithme

Conclusion

## II.1/ Bases minimales et indices de Kronecker

Le noyau  $N$  de  $M$  est vu comme un  $K[x]$ -module

On peut chercher à calculer une **base minimale** de  $N$

$m - r$  vecteurs de degré minimaux les **indices de Kronecker**  $\delta_1, \dots, \delta_{m-r}$

$$\begin{bmatrix} 14x^2 + 9 + 9x^3 + 12x & 3 + 11x^2 + x^3 \\ 11x^3 + 12 + 11x^2 & 13 + 11x^2 + 14x^3 \\ 12 + 4x + x^2 & 14x^2 + 2 + 11x + 11x^3 \\ 1 + 4x^2 + 9x & 12 + 6x^3 + 5x^2 \end{bmatrix}$$

## II.1/ Bases minimales et indices de Kronecker

Le noyau  $N$  de  $M$  est vu comme un  $K[x]$ -module

On peut chercher à calculer une **base minimale** de  $N$

$m - r$  vecteurs de degré minimaux les **indices de Kronecker**  $\delta_1, \dots, \delta_{m-r}$

$$\begin{bmatrix} 5 + \dots + 8x^5 & 7 + \dots + 12x^5 & 9 + \dots + x^5 & 1 \\ 2x + 7 & 8 + 3x & 6 + 2x & 6x + 7 \end{bmatrix} \begin{bmatrix} \dots + 9x^3 & \dots + x^3 \\ \dots + 11x^3 & \dots + 14x^3 \\ \dots + x^2 & \dots + 11x^3 \\ \dots 4x^2 & \dots + 6x^3 \end{bmatrix} \equiv 0$$



## Transfert des degrés

$$\sum_{i=1}^{m-r} \delta_i \leq \text{McMillan-deg}M$$

où le degré de McMillan est le maximum des degrés des déterminants de sous-matrices  $r \times r$  de  $M$

⇒ Une base minimale du noyau a donc une **taille** en  $O(n \times \sum_i \delta_i) = O(\mathbf{n^2d})$

Ingrédients de preuve

$$\begin{bmatrix} D & C \end{bmatrix} \cdot \begin{bmatrix} A \\ B \end{bmatrix} = 0 \Rightarrow D^{-1}C = -BA^{-1}$$

Conservation des **invariants des fractions** (dénominateurs)

## II.2/ Diviser-doubler pour régner

Voir l'algorithme du déterminant [Storjohann] ou de l'inversion générique [Jeannerod, Villard]

On cherche à **diviser la dimension** par deux tout en au plus **doublant les degrés**

$$\Rightarrow \text{Coût en } \sum_{i=1}^{\log n} \left(\frac{n}{2^i}\right)^\omega 2^i d = O(\mathbf{n}^\omega \mathbf{d})$$

Nota. Les diviser pour régner usuels de l'algèbre linéaire — à base de compléments de Schur — sont donc inopérants

## II.3/ Mixte remontée de Hensel / approximation de Padé

$$n + p = n + 1 \quad \left\{ \begin{array}{c} \left[ \begin{array}{c} A \\ \hline b^t \end{array} \right] \end{array} \right.$$

$$n + p = 2n \quad \left\{ \begin{array}{c} \left[ \begin{array}{c} A \\ \hline B \end{array} \right] \end{array} \right.$$

$A$  inversible, noyau de  $M$  :

qd  $p = \mathbf{1}$  **vecteur de degré**  $\delta = \mathbf{nd}$

$$x = b^t A^{-1}$$

$$p\delta = nd, \quad O^{\sim}(\text{MM}(n, d)) \quad [\text{S2003}]$$

qd  $p = \mathbf{n}$  **vecteurs de degré**  $\delta = \mathbf{d}$

$$S^{-1}N = BA^{-1}$$

$$p\delta = nd, \quad O^{\sim}(\text{MM}(n, d)) \quad [\text{GJV2003}]$$

En temps  $\tilde{O}(\text{MM}(n, d))$  **on dispose** :

- ⊙ de **développements**  $BA^{-1}$ ,  $p \times n$ , à l'ordre  $\delta$  si  $p\delta = O(nd)$
- ⊙ d'**approximants**  $p \times p$  à l'ordre  $\delta$  si  $p\delta = O(nd)$

En temps  $O^\sim(\text{MM}(n, d))$  **on dispose** :

- ⊙ de **développements**  $BA^{-1}$ ,  $p \times n$ , à l'ordre  $\delta$  si  $p\delta = O(nd)$
- ⊙ d'**approximants**  $p \times p$  à l'ordre  $\delta$  si  $p\delta = O(nd)$

$\rightsquigarrow$  Gérer le déséquilibre des degrés ?

## II.4/ Empilement de bases minimales

Rang  $n$  et degré  $d$ ,  $n$  vecteurs dans le noyau, puisque  $\sum \delta_i \leq nd$ ,  
**au moins  $n/2$  vecteurs de degré au plus  $2d$**

$$\left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \left[ \begin{array}{c} \\ \\ \\ \end{array} \right] \left. \begin{array}{l} n \\ \\ n \end{array} \right\} = 0$$

## II.4/ Empilement de bases minimales

Rang  $n$  et degré  $d$ ,  $n/2$  vecteurs dans le noyau, puisque  $\sum \delta_i \leq nd$ ,  
**au moins  $n/4$  vecteurs de degré au plus  $4d$**

$$\left[ \begin{array}{c} \text{--- } 4d \text{ ---} \\ \text{--- } 2d \text{ ---} \end{array} \right] \left[ \begin{array}{c} \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \\ \text{--- } \end{array} \right] \left. \begin{array}{c} n \\ \\ \\ \\ \\ \\ \\ \\ n/2 \end{array} \right\} = 0$$



## II.4/ Empilement de bases minimales

Pour  $M$  de degré  $d$ , si  $p$  vecteurs dans le noyau, puisque  $\sum \delta_i \leq nd$ ,  
**au moins  $p/2$  vecteurs de degré au plus  $2nd/p$**

$$\left[ \begin{array}{c} \dots \\ 4d \\ 2d \end{array} \right] \left[ \begin{array}{c} \\ \\ \\ \dots \\ \\ \end{array} \right] \left. \begin{array}{l} n \\ \\ \\ p \end{array} \right\} = 0$$

**Schéma d'algorithme** pour le calcul du **noyau** de  $M \in \mathbb{K}[x]^{2n \times n}$

$p := n$

Tant que  $p \neq 0$

$\delta := 2nd/p$

Extraire une sous-matrice  $\bar{M} \in \mathbb{K}[x]^{(n+p) \times n}$

$N^{(\delta)} :=$  Vecteurs minimaux du noyau  $(\bar{M}, \delta)$

$p := p - \#N^{(\delta)}$

$N := \begin{bmatrix} N^{(\delta)} \\ N \end{bmatrix}$

**Schéma d'algorithme** pour le calcul du **noyau** de  $M \in \mathbb{K}[x]^{2n \times n}$

$p := n$

Tant que  $p \neq 0$

$\delta := 2nd/p$

Extraire une sous-matrice  $\bar{M} \in \mathbb{K}[x]^{(n+p) \times n}$

$\mathbf{N}^{(\delta)} :=$  **Vecteurs minimaux du noyau**  $(\bar{M}, \delta)$   $\longleftarrow$

$p := p - \#\mathbf{N}^{(\delta)}$

$N := \begin{bmatrix} \mathbf{N}^{(\delta)} \\ N \end{bmatrix}$

# Plan de l'exposé

Introduction et contexte

I - Résultats antérieurs

II - Principes de mise en œuvre

**III - Bases minimales compressées**

IV - L'algorithme

Conclusion

## Problème :

Calcul de  $p/2$  vecteurs minimaux de degré au plus  $2nd/p$  dans le noyau de

$$M = \left[ \begin{array}{c} A \\ \hline B \end{array} \right] \begin{array}{l} n \\ p \end{array}$$

## Problème :

Calcul de  $p/2$  vecteurs minimaux de degré au plus  $2nd/p$  dans le noyau de

$$M = \left[ \begin{array}{c} A \\ \hline B \end{array} \right] \begin{array}{l} n \\ p \end{array}$$

## Solution ?

Algorithme d'approximation d'emblée : coût en  $O\tilde{((n/p)n^\omega d)}$  trop élevé

Compresser en gardant les “mêmes solutions” ?

$$\left[ \begin{array}{c|c} BA^{-1} & -I \end{array} \right] \cdot \left[ \begin{array}{c} A \\ \hline B \end{array} \right] = 0$$

Pour une base minimale  $N$  du noyau il existe  $S \in K[x]^{p \times p}$  telle que

$$S \cdot \left[ \begin{array}{c|c} BA^{-1} & -I \end{array} \right] = \left[ \begin{array}{c|c} T & -S \end{array} \right] = N$$

→ On se ramène au cas où une base minimale est partiellement donnée par un **dénominateur  $S$  minimal à gauche** :

$$S^{-1}T = BA^{-1}$$

## Schéma de compression :

**Vecteurs minimaux** de degré au plus  $\delta$  dans le noyau de

$$\left[ \begin{array}{c} A \\ \hline B \end{array} \right] \begin{array}{l} n \\ p \end{array}$$

1. Calcul de  $BA^{-1} \in \mathbb{K}(x)^{p \times n}$
2. Dénominateur minimal  $S$  à gauche :  $S^{-1}T = BA^{-1} \in \mathbb{K}(x)^{p \times n}$
3.  $N := S[BA^{-1} \quad -I]$
4. Lignes de  $N$  telles que  $N_i \cdot M = 0$



## Schéma de compression :

**Vecteurs minimaux** de degré au plus  $\delta$  dans le noyau de

$$\left[ \begin{array}{c} A \\ \hline B \end{array} \right] \begin{array}{l} n \\ p \end{array}$$

1. Calcul de  $BA^{-1} \in \mathbb{K}(x)^{p \times n}$
2. Dénominateur minimal  $S$  à gauche :  $S^{-1}\bar{T} = BA^{-1}\mathbf{P} \in \mathbb{K}(x)^{p \times p}$
3.  $N := S[BA^{-1} \quad -I]$
4. Lignes de  $N$  telles que  $N_i \cdot M = 0$

## Schéma de compression :

**Vecteurs minimaux** de degré au plus  $\delta$  dans le noyau de

$$\left[ \begin{array}{c} A \\ \hline B \end{array} \right] \begin{array}{l} n \\ p \end{array}$$

1. Calcul de  $BA^{-1} \bmod \mathbf{x}^{\eta+1}$
2. Dénominateur minimal  $S$  à gauche :  $S^{-1}\bar{T} = BA^{-1}\mathbf{P} \bmod \mathbf{x}^{\eta+1}$
3.  $N := S[BA^{-1} \quad -I] \bmod \mathbf{x}^{\delta+1}$
4. Lignes de  $N$  telles que  $N_i \cdot M = 0$

## Conditions sur la matrice $P$ de compression :

⊙  $S$  **dénominateur minimal** pour  $BA^{-1}P$  comme pour  $BA^{-1}$

i.e. irréductibilité de  $S^{-1}\bar{T} = BA^{-1}P$

⊙ **Reconstruction** de  $BA^{-1}P$  possible à gauche à l'**ordre**  $\eta = O(\delta)$

$$S^{-1}\bar{T} = BA^{-1}P \text{ mod } x^{\eta+1} \iff S^{-1}\bar{T} = CR^{-1} \text{ mod } x^{\eta+1}$$

$$\iff SC = \bar{T}R \text{ mod } x^{\eta+1}$$

$$\iff SC = \bar{T}R$$

## Proposition :

$\mathbf{P} \in \mathbb{K}[x]^{n \times p}$  **aléatoire** de degré  $d - 1$

- Si  $S^{-1}T = BA^{-1}$  est irréductible alors  $S^{-1}\bar{T} = BA^{-1}P$  est irréductible
- Il existe une description à droite  $BA^{-1}P = CR^{-1}$  de degré  $O(nd/p)$

↔ Ingrédients de preuve

Réalisations de fractions rationnelles [Kai80]

Réurrences linéaires matricielles [Vil97]

**Lemme :**

Soit  $A$  de déterminant de degré  $\nu$ . Il existe  $\sigma : \mathbb{K}[x]^{n \times p} \rightarrow \mathbb{K}[x]^{\nu \times p}$  surjective, ainsi que  $X$ ,  $Q$  et  $A_o$ , telles que pour toute matrice  $P$ ,

$$\mathbf{B}(\mathbf{x})\mathbf{A}(\mathbf{x})^{-1}\mathbf{P}(\mathbf{x}) = \mathbf{Q}(\mathbf{x}) + \mathbf{X}(\mathbf{x} - \mathbf{A}_o)^{-1}\sigma(\mathbf{P}(\mathbf{x})).$$

Si  $P$  (degré  $\leq d - 1$ ) est choisie aléatoirement et uniformément alors  $\sigma(P)$  (sur  $\mathbb{K}$ ) l'est aussi,

# Plan de l'exposé

Introduction et contexte

I - Résultats antérieurs

II - Principes de mise en œuvre

III - Bases minimales compressées

**IV - L'algorithme**

Conclusion

## Calcul probabiliste certifié du noyau de $M \in K[\mathbf{x}]^{m \times n}$

Calcul Monte Carlo du rang  $\rho$

$$M := Q_L M Q_R \in K[x]^{m \times \rho}$$

Si  $\det M_{1..\rho, 1..\rho} = 0$  alors “raté”

Tant que  $p \neq 0$

Seuils de degré / dimension successifs

Vecteurs minimaux du noyau correspondant

Mise à jour de  $N$  : empilement

Si  $N \cdot M \neq 0$  alors “raté”

## Calcul probabiliste certifié du noyau de $M \in K[\mathbf{x}]^{m \times n}$

Calcul Monte Carlo du rang  $\rho$

$$M := Q_L M Q_R \in K[x]^{m \times \rho}$$

Si  $\det M_{1..\rho, 1..\rho} = 0$  alors “raté”

Tant que  $p \neq 0$

Seuils de degré / dimension successifs

Vecteurs minimaux du noyau correspondant

Mise à jour de  $N$  : empilement

**Si  $N \cdot M \neq 0$  alors “raté” ←**



## Ingrédients de preuve

- ↪ **Minimalité** des sous-bases : localisation des degrés dominants  
test explicite de réduction
- ↪ **Indépendance** : par construction des sous-problèmes
- ↪ **Appartenance au noyau** : test  $N \cdot M = 0$
- ↪ **Noyau complet** :  $m - \rho \geq m - r$

## Théorème :

Le rang de  $M \in \mathbb{K}[x]^{n \times n}$  de degré  $d$  ainsi que  $n - r$  vecteurs polynomiaux du noyau se calculent en  $O^{\sim}(\mathbf{MM}(\mathbf{n}, \mathbf{d})) = O^{\sim}(n^{\omega}d)$  opérations dans  $\mathbb{K}$  par un algorithme probabiliste certifié.

Les degrés de ces vecteurs satisfont

$$\sum_{i=1}^{n-r} d_i \leq \log_2(\mathbf{n}) \cdot \text{McMillan-deg}(M).$$

# Plan de l'exposé

Introduction et contexte

I - Résultats antérieurs

II - Principes de mise en œuvre

III - Bases minimales compressées

IV - L'algorithme

**Conclusion**

- ⊙ Calcul d'une base minimale
  - Élimination mi-unimodulaire / mi-rationnelle
  - Deux types d'itération à accorder**
- ⊙ Prolongements
  - Approximation, matrices structurées
  - Inversion** (cas général), **polynôme caractéristique**