Métriques rang et codes de Gabidulin généralisés aux corps de nombres

Daniel AUGOT [1] Pierre LOIDREAU [2,3] Gwezheneg ROBERT [1,2]

[1] LIX – Laboratoire d'informatique de l'École polytechnique
INRIA – Saclay-Île-de-France – Palaiseau, France

[2] IRMAR – Institut de Recherche MAthématique de Rennes
Université de Rennes 1 – Rennes, France

[3] DGA – Direction Générale de l'Armement – Rennes, France

mars 2014

Introduction

- Codes de Gabidulin [Gabidulin, 1984]
  - codes en métrique rang, sur des corps finis
  - codes optimaux : $n + 1 = d + k$
  - existent pour toutes les valeurs de n, k et d
  - algorithmes de décodage efficaces
  - nombreuses utilisations : cryptographie, codage de réseau, codage espace-temps
- Objectifs :
  - donner plusieurs définitions pour la métrique rang
  - donner une construction directe dans des corps de nombres
  - adapter un algorithme de décodage

Plan

θ-polynômes

Pour les codes de Gabidulin :

- $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^m}$
- Frobenius : $x \mapsto x^q$
- q-polynômes :
  $P(X) = \sum_{i=0}^{d} p_i X^{q^i}$, $p_i \in \mathbb{F}_{q^m}$
  - addition composante par composante
  - composition des polynômes
  - $P(\alpha) = \sum p_i \alpha^{q^i}$

θ-polynômes

Pour les codes de Gabidulin :

- $\mathbb{F}_q \hookrightarrow \mathbb{F}_{q^m}$
- Frobenius : $x \mapsto x^q$
- q-polynômes :
  $P(X) = \sum_{i=0}^{d} p_i X^{q^i}$, $p_i \in \mathbb{F}_{q^m}$
  - addition composante par composante
  - composition des polynômes
  - $P(\alpha) = \sum p_i \alpha^{q^i}$

Ici :

- $K \hookrightarrow L$ avec $[L : K] = m$
- $\theta \in Gal(K \hookrightarrow L)$
- θ-polynômes
  $P(X) = \sum_{i=0}^{d} p_i X^i$, $p_i \in L$
  - addition composante par composante
  - $X \cdot a = \theta(a) \cdot X$
  - $P(\alpha) = \sum p_i \theta^i(\alpha)$

Propriétés des θ-polynômes

Définition

On note $L[X;\theta]$ l'ensemble des θ-polynômes.
Il est aussi appelé anneau de Øre. [Øre, 1932, 1933]

Proposition

- $\deg(P \cdot Q) = \deg(P) + \deg(Q)$
- *division euclidienne à gauche et à droite*
- $P(a + \lambda b) = P(a) + \lambda P(b)$, $a, b \in L, \lambda \in K$

Racines d'un θ-polynôme

Définition

Racines d'un θ-polynôme P :
$\mathrm{Roots}(P) = \{\alpha \in L : P(\alpha) = 0\}$.

Remarque

- *θ peut être vu comme une application K-linéaire de L.*
- *L'ensemble des racines est un K-espace vectoriel.*

Théorème

Si le polynôme caractéristique de θ est sans facteur carré, alors pour tout polynôme P non nul,

$$\dim(\mathrm{Roots}(P)) \leqslant \deg(P)$$

Polynômes annulateurs

Théorème

On suppose toujours le polynôme caractéristique de θ sans facteur carré.
Soit $V \subset L$ un sous-K-espace vectoriel de dimension s.
Alors il existe un unique θ-polynôme unitaire $P \in L[X;\theta]$ de degré s tel que

$$\forall v \in V, P(v) = 0$$

(et aucun de degré inférieur).

Définition

Pour $(v_1, \ldots, v_s) \in L^s$, on note $Nul_{[v_1,\ldots,v_s]}$ le polynôme annulateur de $Vect(v_1, \ldots, v_s)$.

Polynômes d'interpolation

Théorème

On suppose toujours le polynôme caractéristique de θ sans facteur carré.
Soient $x_1, \ldots, x_s \in L$ K-linéairement indépendants et $y_1, \ldots, y_s \in L$.
On définit le θ-polynôme :

$$P(X) = \sum_{i=1}^{s} y_i \frac{Nul_{[x_1,\cdots,x_{i-1},x_{i+1},\ldots,x_s]}(X)}{Nul_{[x_1,\cdots,x_{i-1},x_{i+1},\ldots,x_s]}(x_i)}$$

alors

$$\forall 1 \leqslant i \leqslant s,\ P(x_i) = y_i$$

Métriques rang

$$x = (x_1, \ldots, x_n) \in L^n,$$

Définition

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L,
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L, $s = ordre(\theta)$.
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_2(x) = rang_K \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L, $s = ordre(\theta)$.
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_1(x) = rang_L \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_2(x) = rang_K \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L, $s = ordre(\theta)$.
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_0(x) = \deg(Nul_{[x_1,\ldots,x_n]}(X))$$

$$w_1(x) = rang_L \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_2(x) = rang_K \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L, $s = ordre(\theta)$.
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_0(x) = \deg(Nul_{[x_1,\ldots,x_n]}(X))$$

$$w_1(x) = rang_L \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_2(x) = rang_K \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Théorème

$\forall x \in L^n$, *on a*
$w_0(x) = w_1(x)$.

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L, $s = ordre(\theta)$.
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_0(x) = \deg(Nul_{[x_1,\ldots,x_n]}(X))$$

$$w_1(x) = rang_L \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_2(x) = rang_K \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Théorème

$\forall x \in L^n$, *on a*
$w_0(x) = w_1(x)$.

Théorème

$\forall x \in L^n$, *on a*
$w_2(x) = w_3(x)$.

Métriques rang

$(b_1, \ldots, b_m)$ une K-base de L, $s = ordre(\theta)$.
$x = (x_1, \ldots, x_n) \in L^n$, avec $x_i = \sum_j x_{i,j} b_j$.

Définition

$$w_0(x) = \deg(Nul_{[x_1,\ldots,x_n]}(X))$$

$$w_1(x) = rang_L \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_2(x) = rang_K \begin{pmatrix} \theta^0(x_1) & \cdots & \theta^0(x_n) \\ \vdots & \ddots & \vdots \\ \theta^{s-1}(x_1) & \cdots & \theta^{s-1}(x_n) \end{pmatrix}$$

$$w_3(x) = rang_K \begin{pmatrix} x_{1,1} & \cdots & x_{n,1} \\ \vdots & \ddots & \vdots \\ x_{1,m} & \cdots & x_{n,m} \end{pmatrix}$$

Théorème

$\forall x \in L^n$, *on a* $w_0(x) = w_1(x)$.

Théorème

$\forall x \in L^n$, *on a* $w_1(x) \leqslant w_2(x)$, *avec égalité si* $L^\theta = K$.

Théorème

$\forall x \in L^n$, *on a* $w_2(x) = w_3(x)$.

Exemple

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[j] = K \hookrightarrow L = K[\alpha] = K[Y]/(Y^6 - 2) \text{ avec } j^3 = 1$$

$\theta : \alpha \mapsto j\alpha$
La matrice de θ, vu comme application linéaire, est :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & j & 0 & 0 & 0 & 0 \\ 0 & 0 & j^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & j & 0 \\ 0 & 0 & 0 & 0 & 0 & j^2 \end{pmatrix}$$

$\text{Roots}(X^1 - X^0) = \{u + v\alpha^3\}$
La dimension (2) est strictement supérieure au degré (1).

Exemple

$$\mathbb{Q} \hookrightarrow \mathbb{Q}[j] = K \hookrightarrow L = K[\alpha] = K[Y]/(Y^6 - 2) \text{ avec } j^3 = 1$$

$\theta : \alpha \mapsto j\alpha$
La matrice de θ, vu comme application linéaire, est :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & j & 0 & 0 & 0 & 0 \\ 0 & 0 & j^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & j & 0 \\ 0 & 0 & 0 & 0 & 0 & j^2 \end{pmatrix}$$

$\text{Roots}(X^1 - X^0) = \{u + v\alpha^3\}$
La dimension (2) est strictement supérieure au degré (1).

$\theta : \alpha \mapsto (j+1)\alpha$
La matrice de θ, vu comme application linéaire, est :

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & j+1 & 0 & 0 & 0 & 0 \\ 0 & 0 & j & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & j^2 & 0 \\ 0 & 0 & 0 & 0 & 0 & -j \end{pmatrix}$$

La dimension de l'espace des racines d'un θ-polynôme est bornée par son degré.

Plan

Contexte

- On dispose de :
  - $K \hookrightarrow L$, de degré $[L : K] = m$
  - $\theta \in Gal(K \hookrightarrow L)$
- On suppose de plus que (conditions équivalentes) :
  - $Gal(K \hookrightarrow L) =< \theta >$
  - $L^{\theta} = K$
  - le polynôme caractéristique de θ est sans facteur carré
- Ainsi, on a :
  - $w_0 = w_1 = w_2 = w_3 = w$
  - $\forall\, P \neq 0$, $\dim(\text{Roots}(P)) \leqslant \deg(P)$

Codes de Gabidulin généralisés

Définition (Codes de Gabidulin généralisés $Gab_{\theta,k}(g)$)

Soient $k < n \leqslant m$ des entiers et soit $g = (g_1, \ldots, g_n) \in L^n$ une famille K-linéairement indépendante, appelée le support du code.

$$Gab_{\theta,k}(g) = \{(f(g_1), \ldots, f(g_n)) : f \in L[X;\theta], \deg(f) < k\}$$

Codes MRD

Proposition (Borne de Singleton)

Soit $\mathcal{C}$ un code linéaire de longueur n, de dimension k et de distance minimale (en métrique rang) d. Alors

- $d \leqslant n - k + 1$
- $d \leqslant \frac{m}{n}(n-k) + 1$

Définition

Quand $d = n - k + 1$, on dit que le code $\mathcal{C}$ est un code MRD (Maximum Rank Distance).

Proposition

Les codes de Gabidulin généralisés sont des codes MRD.

Décodage

Étant donnés

- *un code de Gabidulin généralisé*
  - $[n, k, d]$ *et* t*-correcteur*
  - *de support* $(g_1, \ldots, g_n)$
- *un mot reçu* $(y_1, \ldots, y_n)$

Décodage

Étant donnés

- *un code de Gabidulin généralisé*
  - $[n, k, d]$ *et* t*-correcteur*
  - *de support* $(g_1, \ldots, g_n)$
- *un mot reçu* $(y_1, \ldots, y_n)$

Définition (*Decodage*)

Trouver f *et* $e \in L^n$*, tels que :*

- $\forall i \; y_i = f(g_i) + e_i$
- $\deg(f) < k$
- $w(e) \leqslant t$

Décodage

Étant donnés

- *un code de Gabidulin généralisé*
  - $[n, k, d]$ *et* t*-correcteur*
  - *de support* $(g_1, \ldots, g_n)$
- *un mot reçu* $(y_1, \ldots, y_n)$

Définition (*Decodage*)

Trouver f *et* $e \in L^n$*, tels que :*

- $\forall i \; y_i = f(g_i) + e_i$
- $\deg(f) < k$
- $w(e) \leqslant t$

Définition (*Reconstruction*1)

Trouver (V, f) *tel que :*

- $\forall i \; V(y_i) = (V \cdot f)(g_i)$
- $0 \leqslant \deg(V) \leqslant t$
- $\deg(f) < k$

Décodage

Étant donnés

- *un code de Gabidulin généralisé*
  - $[n, k, d]$ *et* t*-correcteur*
  - *de support* $(g_1, \ldots, g_n)$
- *un mot reçu* $(y_1, \ldots, y_n)$

Définition (*Decodage*)

Trouver f *et* $e \in L^n$*, tels que :*

- $\forall i\ y_i = f(g_i) + e_i$
- $\deg(f) < k$
- $w(e) \leqslant t$

Définition (*Reconstruction1*)

Trouver (V, f) *tel que :*

- $\forall i\ V(y_i) = (V \cdot f)(g_i)$
- $0 \leqslant \deg(V) \leqslant t$
- $\deg(f) < k$

Définition (*Reconstruction2*)

Trouver (W, N) *tel que :*

- $\forall i\ W(y_i) = N(g_i)$
- $0 \leqslant \deg(W) \leqslant t+1$
- $\deg(N) < k + t+1$

Décodage

Théorème

Si

- *il existe une solution* (V, f)
- *on connaît une solution* (W, N)
- $t \leqslant \lfloor \frac{n-k}{2} \rfloor$

Alors $f = W \backslash N$

Définition (*Decodage*)

Trouver f *et* $e \in L^n$, *tels que :*

- $\forall i \; y_i = f(g_i) + e_i$
- $\deg(f) < k$
- $w(e) \leqslant t$

Définition (*Reconstruction1*)

Trouver (V, f) *tel que :*

- $\forall i \; V(y_i) = (V \cdot f)(g_i)$
- $0 \leqslant \deg(V) \leqslant t$
- $\deg(f) < k$

Définition (*Reconstruction2*)

Trouver (W, N) *tel que :*

- $\forall i \; W(y_i) = N(g_i)$
- $0 \leqslant \deg(W) \leqslant t+1$
- $\deg(N) < k + t+1$

Plan

Résolution par un pivot de Gauss

Cela consiste à résoudre le système suivant, dont les inconnues sont les coefficients de N et W.

$$\begin{pmatrix} g_1 & \cdots & \theta^{k+t-1}(g_1) & y_1 & \cdots & \theta^t(y_1) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ g_n & \cdots & \theta^{k+t-1}(g_n) & y_n & \cdots & \theta^t(y_n) \end{pmatrix} \cdot \begin{pmatrix} n_0 \\ \vdots \\ n_{k+t-1} \\ -w_0 \\ \vdots \\ -w_t \end{pmatrix} = 0$$

Matrice à n lignes et
$n+1$ colonnes quand $n-k$ est pair
$n+2$ colonnes quand $n-k$ est impair
$\Longrightarrow$ toujours une solution.

ici, $n-k$ est pair

Le Trickier Algorithm [Loidreau, 2005]

But : trouver (N_0, W_0) et (N_1, W_1) solutions de *Reconstruction2*

- à l'initialisation :
  - ▷ on a $N_j(g_i) = W_j(y_i)$ pour $1 \leqslant i \leqslant k$ et $j = 0, 1$
  - ▷ $\deg(W) \sim 0$ et $\deg(N) \sim k - 1$
- à chaque itération ($n - k$ fois) :
  - ▷ on obtient $N_j(g_i) = W_j(y_i)$ pour un nouvel indice i et $j = 0, 1$
  - ▷ le degré d'un des couples augmente de 1, l'autre ne change pas
- à la fin :
  - ▷ on a $N_j(g_i) = W_j(y_i)$ pour $1 \leqslant i \leqslant n$ et $j = 0, 1$
  - ▷ $\deg(W) \sim t$ et $\deg(N) \sim t + k - 1$

Complexité des algorithmes

- Complexité :
  - avec l'élimination de Gauss : $O(n^3)$
  - avec le Trickier Algorithm : $O(n^2)$
- Temps de calcul :
  - En pratique, le Trickier Algorithm est plus rapide que le pivot de Gauss quand $k \leqslant \frac{n}{2}$

- Problème : la taille des coefficients, qui augmente exponentiellement
- Solution : calculer dans un quotient. Pour cela, on choisit un idéal premier $\mathfrak{p}$. On fera alors les calculs dans un corps fini.

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & L \\ | & & | \\ \mathbb{Z} & \hookrightarrow & \mathcal{O}_L \\ | & & | \\ p\mathbb{Z} & \hookrightarrow & \mathfrak{p} \\ \vdots & & \vdots \\ \mathbb{Z}/p\mathbb{Z} & \hookrightarrow & \mathcal{O}_L/\mathfrak{p} \end{array}$$

Merci de votre attention.

Trickier Algorithm (détails)

- Initialisation
  - $ANN(X)$ est le polynôme annulateur de $(g_1, \ldots, g_k)$
  - $INT(X)$ est le polynôme interpolateur de $((g_1, y_1), \ldots, (g_k, y_k))$
  - $N_0(X) = ANN(X)$
  - $W_0(X) = 0$
  - $N_1(X) = \lambda INT(X)$
  - $W_1(X) = \lambda X^0$

Trickier Algorithm (détails)

- Iterations ($n-k$ fois)
  - on calcule les défauts :
    - $u_0 \longleftarrow W_0(y_i) - N_0(g_i)$
    - $u_1 \longleftarrow W_1(y_i) - N_1(g_i)$
  - puis on échange :
    - $u_0 \longleftrightarrow u_1$
    - $N_0 \longleftrightarrow N_1$
    - $W_0 \longleftrightarrow W_1$
  - puis on effectue une mise à jour des polynômes :
    - $N_0 \longleftarrow u_0\theta(N_0) - \theta(u_0)N_0$
    - $W_0 \longleftarrow u_0\theta(W_0) - \theta(u_0)W_0$
    - $N_1 \longleftarrow u_0 N_1 - u_1 N_0$
    - $W_1 \longleftarrow u_0 W_1 - u_1 W_0$

    (autres formules si $u_0 = 0$ ou $u_1 = 0$)

Trickier Algorithm (détails)

Il y a 4 mises à jour possibles :

		nouveau N_0	nouveau N_1
$u_0 \neq 0$	$u_1 \neq 0$	$u_0\theta(N_0) - \theta(u_0)N_0$	$u_0 N_1 - u_1 N_0$
$u_0 \neq 0$	$u_1 = 0$	$u_0\theta(N_0) - \theta(u_0)N_0$	N_1
$u_0 = 0$	$u_1 = 0$	$\theta(N_0)$	N_1
$u_0 = 0$	$u_1 \neq 0$	$\theta(N_0)$	N_0

Évolution de la taille des coefficients au cours du TA

valeurs calculées, pas de simplification					
N_0	W_0	N_1	W_1	u_0	u_1
3	1	24	22	3	25
51	49	26	26	50	26
56	56	80	79	58	81
165	164	140	139	166	143
285	284	310	310	287	311
622	621	602	601	623	602
1202	1201	1230	1229	1202	1229
2456	2455	2434	2433	2456	2435
4867	4865	4890	4889		

valeurs théoriques					
N_0	W_0	N_1	W_1	u_0	u_1
3	1	24	22	15	35
66	64	46	44	78	58
111	109	131	129	123	143
281	279	261	259	293	273
541	539	561	559	553	573
1141	1139	1121	1119	1153	1133
2261	2259	2281	2279	2273	2293
4581	4579	4561	4559	4593	4573
9141	9139	9161	9159		

valeurs calculées, simplifiées par le PGCD					
N_0	W_0	N_1	W_1	u_0	u_1
3	1	12	11	3	12
22	21	14	13	22	13
23	21	34	32	22	32
64	63	51	50	64	52
100	99	113	112	99	112
223	221	210	208	223	210
417	415	430	429	416	430
849	847	841	840	850	841
1660	1658	1687	1685		

Temps de calcul

			TA				PG		taille coefficients	
n	k	t	précalcul	initialisation	boucle	division	pivot	division	TA	PG
16	2	7	0	0	0.220	0.360	2.520	0.010	2 144	7 365
	4	6	0.010	0.010	0.540	10.580	20.420	0.010	16 446	14 716
	6	5	0.050	0.020	0.380	8.080	20.060	0.010	11 565	14 701
	8	4	0.150	0.030	0.440	13.240	19.920	0.020	15 129	12 711
	10	3	0.330	0.100	0.430	20.070	19.830	0.020	15 639	14 696
	12	2	0.580	0.520	0.400	26.120	19.410	0.020	16 982	12 671
	14	1	1.170	5.330	0.410	36.190	19.750	0.020	19 075	12 669
	16	0	3.120	52.400	0	58.190	19.560	0.010	24 356	12 666