

# Codes quasi-cycliques sur des anneaux de matrices

Pierre-Louis Cayrel/Christophe Chabot/Abdelkader Necer

Université de Limoges - XLIM - DMI - PI2C

Séminaire PI2C Limoges - 03/03/2009

# Sommaire

- 1 Introduction
- 2 SRL à coefficients matriciels
  - Action de  $M_{\ell,\ell}(\mathbb{F}_q)[X]$  sur  $(\mathbb{F}_q^\ell)^\mathbb{N}$
  - Résultats principaux
  - Application aux codes
- 3 Codes quasi-cycliques
  - Action de  $M_{\ell,\ell}(\mathbb{F}_q)[X]$  sur  $(\mathbb{F}_q^\ell)^m$
  - Construction de  $\Omega(P)$ -codes
- 4 Construction de codes autoduaux
  - Codes autoduaux Euclidiens
  - Codes autoduaux Hermitiens

# Introduction

## Définition

Un code de dimension  $k$  et de longueur  $n$  sur  $\mathbb{F}_q$  (ou un  $[n, k]$ -code sur  $\mathbb{F}_q$ ) est un sous-espace vectoriel de dimension  $k$  de  $\mathbb{F}_q^n$ .

## Définition

Poids d'un mot  $c$  :

$$w(c) := \#\{i \in \{1, \dots, n\} \mid c_i \neq 0\}$$

Distance minimale d'un code  $C$  :

$$d := \min_{c \in C, c \neq 0} w(c)$$

On parle alors de  $[n, k, d]$ -code sur  $\mathbb{F}_q$ .

## Introduction

★ Matrice génératrice :

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

### Définition

Soit  $\langle \cdot, \cdot \rangle$  une application bilinéaire (symétrique). On définit le dual d'un  $[n, k]$ -code  $C$  sur  $\mathbb{F}_q$  par :

$$C^\perp := \{x \in \mathbb{F}_q^n \mid \forall c \in C, \langle x, c \rangle = 0\}$$

$C^\perp$  est un  $[n, n - k]$ -code sur  $\mathbb{F}_q$ .

# Introduction

## Définition

Soit  $C$  un  $[n, k]$ -code. Soit  $\ell$  divisant  $n$  ( $n = m\ell$ ).  
 $C$  est dit quasi-cyclique si

$$\forall c \in C, \quad T^\ell(c) \in C$$

où  $T$  est le shift circulaire :  $T(x_1, x_2, \dots, x_n) := (x_n, x_1, \dots, x_{n-1})$ .

$$G = \begin{pmatrix} A & B & C & 0 \\ 0 & A & B & C \end{pmatrix}$$

$A, B, C$  de taille  $\ell \times \ell$ .

# Introduction

★ Autre représentation :

Un code sera dit quasi-cyclique s'il est stable par :

$S$  :

$((x_1, x_2, \dots, x_\ell), (x_{\ell+1}, x_{\ell+2}, \dots, x_{2\ell}), \dots, (x_{(m-1)\ell+1}, x_{(m-1)\ell+2}, \dots, x_n))$

$\mapsto$

$((x_\ell, x_1, \dots, x_{\ell-1}), (x_{2\ell}, x_{\ell+1}, \dots, x_{2\ell-1}), \dots, (x_n, x_{(m-1)\ell+1}, \dots, x_{n-1}))$

$$G = \begin{pmatrix} A & B & C \\ D & E & F \end{pmatrix}$$

$A, B, C, D, E, F$  de taille  $m \times m$ .

## Motivation

$$G = \begin{pmatrix} A & B & C & 0 \\ 0 & A & B & C \end{pmatrix}$$

**Codes cycliques :**

Si  $X^n - 1 = f(X)g(X)$ , alors  $\langle f(X) \rangle^\perp = \langle g^*(X) \rangle$ .

## Motivation

$$G = \begin{pmatrix} A & B & C & 0 \\ 0 & A & B & C \end{pmatrix}$$

### **Codes cycliques :**

Si  $X^n - 1 = f(X)g(X)$ , alors  $\langle f(X) \rangle^\perp = \langle g^*(X) \rangle$ .

### **Codes quasi-cycliques :**

Si  $X^m - 1 = f(X)g(X)$ , alors  $\Omega(f)^\perp = \Omega({}^t g^*)$ .

## Action de $M_{\ell,\ell}(\mathbb{F}_q)$ sur $(\mathbb{F}_q^\ell)^\mathbb{N}$

Considérons ici des suites d'éléments de  $\mathbb{A} = \mathbb{F}_q^\ell$ .

Notons  $M = M_{\ell,\ell}[\mathbb{F}_q]$ .

**Structure de  $M[X]$ -module à gauche sur  $\mathbb{A}^\mathbb{N}$  :**

$$\begin{aligned}
 M[X] \times \mathbb{A}^\mathbb{N} &\longrightarrow \mathbb{A}^\mathbb{N} \\
 (P(X), V) &\longmapsto P * V := \left( \sum_{i=0}^{\deg(P)} p_i v_{n+i} \right)_{n \in \mathbb{N}} \\
 &= \sum_{i=1}^n p_i T^i(V).
 \end{aligned}$$

où  $P(X) = \sum_{i=0}^{\deg(P)} p_i X^i$ .

# Suites récurrentes linéaires à coefficients matriciels

## Définition

Une suite  $(u_n)_{n \in \mathbb{N}}$  d'éléments de  $\mathbb{F}_q^\ell$  sera dite récurrente linéaire à coefficients matriciels s'il existe  $A_0, \dots, A_{h-1} \in M_{\ell, \ell}[\mathbb{F}_q]$  telles que :

$$u_{n+h} = A_{h-1}u_{n+h-1} + \dots + A_0u_n, \forall n \geq 0.$$

$P(X) = X^h - \sum_{i=0}^{h-1} A_i X^i$  est le polynôme caractéristique de  $u$ .

## Définition

$$\text{Ann}(E) := \{P \in M[X] / \forall u \in E, P * u = 0\}$$

$$\Omega(f) := \{u \in (\mathbb{F}_q^\ell)^\mathbb{N} / f * u = 0\}.$$

## Résultats principaux

Soit  $(u_n)_{n \in \mathbb{N}}$  une SRL de polynôme caractéristique

$$P(X) = X^h + \sum_{i=0}^{h-1} A_i X^i. \text{ Alors :}$$

$$G = \begin{pmatrix} 0 & I_\ell & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & I_\ell \\ -A_0 & -A_1 & \cdots & -A_{h-1} \end{pmatrix} \text{ vérifie :}$$

$$\begin{pmatrix} u_n \\ \vdots \\ u_{n+h-1} \end{pmatrix} = G^n \begin{pmatrix} u_0 \\ \vdots \\ u_{h-1} \end{pmatrix}.$$

## Polynôme caractéristique

### Proposition

Le polynôme caractéristique de  $G$  est donné par la formule :

$$\det(XI_{h\ell} - G) = \det\left(X^h I_\ell + \sum_{i=0}^{h-1} X^i A_i\right).$$

Exemple :  $\ell = 2, h = 3$  sur  $\mathbb{F}_2$

$$\det \left( \begin{pmatrix} X & & & & & \\ & X & & & & \\ & & X & & & \\ & & & X & & \\ & & & & X & \\ & & & & & X \end{pmatrix} - \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \right)$$

$$= \det \begin{pmatrix} X^3 + X^2 + X + 1 & 1 \\ X^2 + X + 1 & X^3 + X^2 + X + 1 \end{pmatrix}$$

## Théorème

Soient  $u \in (\mathbb{F}_q^\ell)^\mathbb{N}$  et  $U(X) \in \mathbb{F}_q^\ell[[X]]$  sa série génératrice.  
 $u$  est une SRL  $\iff U(X)$  est une fraction rationnelle

Remarques :

- $U(X) = \frac{R(X)}{Q(X)}$  avec  $R(X) \in \mathbb{F}_q^\ell[X]$  et  $Q(X) \in M[X]$  avec  $\deg(R) < \deg(Q)$  et  $Q(0)$  inversible.
- $Q(X) * U(X) = R(X)$

## Application aux codes

### Proposition

Soit  $f \in M[X]$  réversible. Alors, il existe  $e \in \mathbb{N}^*$  tel que :

$$f \text{ divise } X^e - 1.$$

Notons  $\mathcal{C}(f) := \{u = (u_0, \dots, u_{e-1}, u_0, \dots, u_{e-1}, \dots) / f * u = 0\}$ .

### Corollaire

$\mathcal{C}(f)$  est un code cyclique sur  $\mathbb{F}_q^\ell$

## Codes quasi-cycliques

Soit  $n = m\ell$ . On considère l'identification :

$$\begin{aligned} \phi : \quad \mathbb{F}_q^{n=m\ell} &\longrightarrow (\mathbb{F}_q^\ell)^m =: \mathbb{A}^m \\ (c_0, \dots, c_{n-1}) &\longmapsto ((c_0, \dots, c_{\ell-1}), \dots, (c_{(m-1)\ell}, \dots, c_{n-1})) \end{aligned}$$

$C \subset \mathbb{F}_q^{m\ell}$  est  $\ell$ -quasi-cyclique  $\iff \phi(C) \subset (\mathbb{F}_q^\ell)^m$  est cyclique.

Soit  $M := M_{\ell, \ell}(\mathbb{F}_q)$ .

**Structure de  $M[X]$  module à gauche :**

$$M[X] \times \mathbb{A}^{\mathbb{N}} \longrightarrow \mathbb{A}^{\mathbb{N}}$$

$$(P(X), V) \longmapsto P * V := \left( \sum_{i=0}^{\deg(P)} p_i v_{n+i} \right)_{n \in \mathbb{N}}$$

$$M[X] \times \mathbb{A}^m \longrightarrow \mathbb{A}^m$$

$$(P(X), c) \longmapsto P * c := \left( \sum_{i=0}^{\deg(P)} p_i c_{(n+i \bmod m)} \right)_{n=0, \dots, m-1}$$

où  $P(X) = \sum_{i=0}^{\deg(P)} p_i X^i$ ,  $V = (v_n)_{n \in \mathbb{N}}$  et  $c = (c_0, \dots, c_{m-1})$ .

## Définition

Soient  $f \in M[X]/\langle X^m - 1 \rangle$  et  $C$  un  $\mathbb{F}_q$ -ss-e.v. de  $\mathbb{A}^m$ .

On note :

- $\Omega(f) := \{x \in \mathbb{A}^m / f * x = 0\}$  ( $\mathbb{F}_q$ -espace vectoriel).
- $Ann(C) := \{P \in M[X]/\langle X^m - 1 \rangle / P * c = 0, \forall c \in C\}$   
(idéal à gauche de  $M[X]/\langle X^m - 1 \rangle$ ).

## Résultats principaux



- $M[X]$  est non commutatif.
- $\text{Ann}(C)$  peut contenir un polynôme de degré minimal non réversible.

### ▷ Résultats négatifs :

- $\text{Ann}(C)$  n'est pas forcément principal.
- En général,  $\Omega(\text{Ann}(C)) \neq C$ .

## Résultats principaux

### ▷ Résultats positifs :

Dans cette section, on considère  $f, Q \in M[X]/\langle X^m - 1 \rangle$  réversibles tels que  $fQ = X^m - 1$ .

$$\dim_{\mathbb{F}_q}(\Omega(f)) = \ell \deg(f).$$

→ Réponse impulsionnelle.

$$\text{Ann}(\Omega(f)) = \langle f \rangle.$$

→  $\text{Ann}(\Omega(f))$  ne contient pas de polynôme de degré inférieur à  $\deg(f)$ .

## Construction de $\Omega(P)$ -codes

### Proposition

$$\Omega(f) = Q * \mathbb{A}^m.$$

- $(Q * e_{i,j})_{i=0,\dots,\deg(f)-1, j=0,\dots,l-1}$  est une famille libre.
- dimension.

### Corollaire

Si  $X^m - 1 = PQ$ , alors, une matrice génératrice de  $\Omega(P)$  est :

$$G_{\Omega(P)} = \begin{pmatrix} {}^tq_0 & {}^tq_1 & {}^tq_2 & \cdots & {}^tq_{\deg Q} & 0 & 0 & \cdots & 0 \\ 0 & {}^tq_0 & {}^tq_1 & \cdots & {}^tq_{\deg Q-1} & {}^tq_{\deg(Q)} & 0 & \cdots & 0 \\ & & \cdots & & & & \cdots & & \end{pmatrix}$$

## Avec longueur prescrite

**Input** :  $\ell, m, deg_{max}$

**Algorithm** :

$list_{poly} \leftarrow [ ];$

for  $d$  from 1 to  $deg_{max}$  do

  for  $P \in \mathbb{M}_{\ell, \ell}(\mathbb{F}_q)[X]$  monic of degree  $d$  do

    if  $P$  divides  $X^m - 1$  then Add  $P$  into  $list_{poly}$  ;

  end for ;

end for ;

**Output** :  $list_{poly}$

## Avec dimension prescrite

**Input :**  $\ell, deg, nb_{steps}$

**Algorithm :**

$list \leftarrow [ ]$ ;

for  $i$  from 1 to  $nb_{steps}$  do

    Pick a random reversible polynomial  $P \in \mathbb{M}_{\ell, \ell}(\mathbb{F}_q)[X]$   
    of degree  $deg$ ;

    Compute  $m$  its exponent;

    Add  $[P, m]$  into  $list$ ;

end for;

**Output :**  $list$

# Codes auto-duaux Euclidiens

## Définition

Considérons le produit scalaire Euclidien :

$$\forall a = (a_1, \dots, a_n), \forall b = (b_1, \dots, b_n), \quad \langle a, b \rangle_e = \sum_{i=1}^n a_i b_i$$

## Théorème

$$\Omega(f)^\perp = \Omega({}^t Q^*).$$

- proposition précédente.
- étaler les calculs...

Codes cycliques :  $X^n - 1 = g(X)h(X)$ ,  $\langle g(X) \rangle^\perp = \langle h^*(X) \rangle$ .

# Construction

- $m = 2m'$
- On cherche  $P$  de degré  $m'$  tels que :  $X^m - 1 = P \cdot {}^t P^*$   
→  $\ell^2 m$  équations de degré 2 à  $\ell^2 m'$  variables.
- Si on suppose que  $P = {}^t P^*$   
→  $\ell^2 m$  équations de degré 2 à  $\ell^2 m'/2$  variables.

Codes autoduaux Euclidiens sur  $\mathbb{F}_4$ 

$n$	Meilleure borne	Meilleure distance	Nombre de codes
8	4	<b>4</b>	2 *
12	6	4	2
16	6	<b>6</b>	3
20	8	7	2
24	8-10	<b>8</b>	9
28	9-11	<b>9</b>	2 *
32	10-12	<b>10</b>	8
36	10-14	<b>10</b>	22
40	12-16	<b>12</b>	8

# Codes autoduaux Hermitiens

## Définition

Sur  $\mathbb{F}_4$ , considérons le produit scalaire Hermitien :

$$\forall a = (a_1, \dots, a_n), \forall b = (b_1, \dots, b_n),$$

$$\langle a, b \rangle_h = \sum_{i=1}^n a_i \theta(b_i) = \sum_{i=1}^n a_i b_i^2$$

## Théorème

$$\Omega(f)^\perp = \Omega(\theta({}^t Q^*)).$$

# Construction

- $m = 2m'$
- On cherche  $P$  de degré  $m'$  tels que :  $X^m - 1 = P.\theta({}^t P^*)$   
→  $\ell^2 m$  équations de degré 3 à  $\ell^2 m'$  variables.
- Si on suppose que  $P = \theta({}^t P^*)$   
→ pas de bons résultats.

# Codes auto-duaux Euclidiens sur $\mathbb{F}_4$

$n$	Meilleure borne	Meilleure distance	Nombre de codes
8	4	<b>4</b>	1
12	4	<b>4</b>	1
16	6	<b>6</b>	1
20	8	<b>8</b>	1
24	8	<b>8</b>	7
28	10	<b>10</b>	2

## Conclusion et perspectives

- Sous-famille de codes quasi-cycliques
  - Représentables par des polynômes à coefficients matriciels.
  - Constructions effectives.
  - Codes auto-duaux avec de bons paramètres.
- 
- Améliorer la factorisation de  $X^m - 1$ .
  - Algorithme de décodage.