

# Codes sur les anneaux de polynômes tordus

Delphine Boucher, Willi Geiselmann, Patrick Solé et Felix Ulmer

Séminaire algo, INRIA Rocquencourt, 5 mai 2008

**Introduction.**

**Codes  $\theta$ -cycliques et  $\theta$ -centraux sur  $\mathbb{F}_q$ .**

**Codes  $\theta$ -cycliques auto-duaux sur  $\mathbb{F}_q$ .**

**Un peu de décodage.**

**Codes tordus sur  $GR(4^2)$ .**

**Bibliographie.**

## Principe.

$$\begin{array}{ccccc}
 \textit{source} & & \textit{canal} & & \textit{but} \\
 m \in F^k & \rightarrow & c \in F^n & \xrightarrow[e \in F^n]{} & c' = c + e \rightarrow m' = m?
 \end{array}$$

Code linéaire  $C$  sur  $F = \mathbb{F}_q$  de longueur  $n$  et de dimension  $k$  :

$$C \subset \mathbb{F}_q^n, \dim(C) = k$$

## Premières définitions.

- Distance de Hamming,  $d$  sur  $\mathbb{F}_q^n$  :

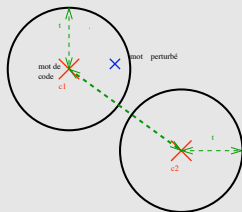
$$d(x, y) = \text{card}(\{i : x_i \neq y_i\}) \text{ pour } x, y \in \mathbb{F}_q^n$$

- Distance minimale  $d$  de  $C$  :

$$d = \min_{x \neq 0} \underbrace{d(x, 0)}_{\text{poids}}$$

- Notation :  $[n, k, d]$
- Capacité de correction :

$$t = E\left(\frac{d-1}{2}\right)$$



Exemple : code contrôle de parité [4, 3, 2].

$$C = \{m G, m \in \mathbb{F}_2^3\}$$

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

$$m \in \mathbb{F}_2^3 \rightarrow c = (m_1, m_2, m_3, m_1 + m_2 + m_3)$$

$$(1, 0, 1) \rightarrow (1, 0, 1, 0) \quad \text{—————} \quad (1, 1, 1, 0) \rightarrow ?$$

## Codes cycliques.

Code linéaire  $C$  de longueur  $n$  sur  $\mathbb{F}_q$  **cyclique** :

$$(a_0, a_1, \dots, a_{n-1}) \in C \Rightarrow (a_{n-1}, a_0, a_1, \dots, a_{n-2}) \in C$$

Représentation polynomiale.

$$\begin{aligned} C(x) &= \{a_0 + a_1x + \dots + a_{n-1}x^{n-1}, a \in C\} \subset \mathbb{F}_q[x]/(x^n - 1) \\ &= (g(x))/(x^n - 1) \text{ idéal de } \mathbb{F}_q[x]/(x^n - 1) \end{aligned}$$

où  $g(x) \mid x^n - 1$ .

Dimension :  $k = n - \deg(g)$

**Codes  $\theta$ -cycliques sur  $\mathbb{F}_q$ .**

[BGU]

Soit  $\theta \in \text{Aut}(\mathbb{F}_q)$ .

Code linéaire  $C$  de longueur  $n$  sur  $\mathbb{F}_q$   $\theta$ -cyclique :

$$(a_0, a_1, \dots, a_{n-1}) \in C \Rightarrow (\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})) \in C.$$

Représentation polynomiale ?

## Anneaux de polynômes tordus.

Soit  $\theta \in \text{Aut}(\mathbb{F}_q)$  d'ordre  $m$ .

$\mathbb{F}_q[x, \theta]$  anneau de polynômes 'tordus'

Addition : comme dans  $\mathbb{F}_q[x]$

Multiplication :  $x a = \theta(a) x$ ,  $a \in \mathbb{F}_q$ .

$\mathbb{F}_q[x, \theta]$  anneau euclidien à droite et à gauche.

Idéal bilatère de  $\mathbb{F}_q[x, \theta]$  :  $(f)$  où  $f \in x^t \mathbb{F}_q^\theta[x^m]$

$\mathbb{F}_q[x, \theta]/(f)$  possède des idéaux principaux à droite et à gauche.

Exemple :  $\mathbb{F}_4[x, \theta]$  avec  $\theta : a \mapsto a^2$  et  $\mathbb{F}_4^\theta = \mathbb{F}_2$

Codes  $\theta$ -cycliques sur  $\mathbb{F}_q$ .

[BGU]

Soit  $\theta \in \text{Aut}(\mathbb{F}_q)$  d'ordre  $m$ .

Code linéaire  $C$  de longueur  $n$  sur  $\mathbb{F}_q$   $\theta$ -cyclique :

$$(a_0, a_1, \dots, a_{n-1}) \in C \Rightarrow (\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})) \in C.$$

Représentation polynomiale ?

Codes  $\theta$ -cycliques sur  $\mathbb{F}_q$ .

[BGU]

Soit  $\theta \in \text{Aut}(\mathbb{F}_q)$  d'ordre  $m$ .

Code linéaire  $C$  de longueur  $n$  sur  $\mathbb{F}_q$   $\theta$ -cyclique :

$$(a_0, a_1, \dots, a_{n-1}) \in C \Rightarrow (\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})) \in C.$$

Représentation polynomiale ?

Hyp :  $n$  multiple de  $m$

Codes  $\theta$ -cycliques sur  $\mathbb{F}_q$ .

[BGU]

Soit  $\theta \in \text{Aut}(\mathbb{F}_q)$  d'ordre  $m$ .

Code linéaire  $C$  de longueur  $n$  sur  $\mathbb{F}_q$   $\theta$ -cyclique :

$$(a_0, a_1, \dots, a_{n-1}) \in C \Rightarrow (\theta(a_{n-1}), \theta(a_0), \dots, \theta(a_{n-2})) \in C.$$

Représentation polynomiale ?

Hyp :  $n$  multiple de  $m$

$$C(x) = (g(x))/(x^n - 1) \text{ idéal à gauche de } \mathbb{F}_q[x, \theta]/(x^n - 1)$$

où  $g(x) \mid_r x^n - 1$ .

**Exemple : codes  $\theta$ -cycliques  $[4, 2]$  sur  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$  avec  $\theta : a \mapsto a^2$ .**

[BGU]

Sur  $\mathbb{F}_4[x, \theta]$  :

$x^4 - 1$  : 15 factorisations en polynômes unitaires de degré 1  
 : 7 facteurs à droite unitaires de degré 2

$$\begin{aligned} x^4 - 1 &= (x^2 + \alpha^2 x + \alpha^2)(x^2 + \alpha^2 x + \alpha) \\ &= \dots \end{aligned}$$

2 codes  $[4, 2]$   $\theta$ -cycliques non équivalents :

$$\begin{array}{ll} (x^2 + 1)/(x^4 - 1) & \text{cyclique} \\ (x^2 + \alpha^2 x + \alpha)/(x^4 - 1) & \text{non cyclique} \end{array}$$

**Exemple : codes  $\theta$ -cycliques  $[4, 2]$  sur  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$  avec  $\theta : a \mapsto a^2$ .**

[BGU]

Sur  $\mathbb{F}_4[x, \theta]$  :

$x^4 - 1$  : 15 factorisations en polynômes unitaires de degré 1  
 : 7 facteurs à droite unitaires de degré 2

$$\begin{aligned} x^4 - 1 &= (x^2 + \alpha^2 x + \alpha^2)(x^2 + \alpha^2 x + \alpha) \\ &= \dots \end{aligned}$$

2 codes  $[4, 2]$   $\theta$ -cycliques non équivalents :

$(x^2 + 1)/(x^4 - 1)$	<i>cyclique</i>	4, 2, 2
$(x^2 + \alpha^2 x + \alpha)/(x^4 - 1)$	<i>non cyclique</i>	4, 2, 3

## Brève comparaison avec les codes de Gabidulin ([G])

$\theta : a \mapsto a^{q_0}$ , automorphisme de Frobenius

$$\mathbb{F}_q^\theta = \mathbb{F}_{q_0} \subset \mathbb{F}_q$$

Isomorphisme entre l'anneau des **polynômes tordus** et l'anneau des **polynômes linéarisés** :

$$\begin{cases} \mathbb{F}_q[x, \theta] & \rightarrow & \mathbb{F}_q[Y^{q_0}, \circ] \\ x & \mapsto & Y^{q_0} \end{cases}$$

Codes de Gabidulin ([G]) : définis sur l'anneau des polynômes linéarisés.

Codes  $\theta$ -centraux sur  $\mathbb{F}_q$ .

Soit  $\theta \in \text{Aut}(\mathbb{F}_q)$  d'ordre  $m$ .

Un code linéaire  $C$  sur  $\mathbb{F}_q$  est un **code  $\theta$ -central** (ou  **$\theta$ -code**) si

$$C(x) = (g(x))/(f(x)) \in \mathbb{F}_q[x, \theta]/(f(x))$$

où

- $f \in Z(\mathbb{F}_q[x, \theta]) = \mathbb{F}_q^\theta[x^m]$ ;
- $g \mid_r f$ .

$$n = \deg(f),$$

$$k = n - \deg(g)$$

**Exemple : codes  $\theta$ -centraux  $[4, 2]$  sur  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$  avec  $\theta : a \mapsto a^2$ .**

[BGU]

$$\begin{array}{ll}
 x^4 - 1 & : \text{ 7 facteurs à droite de degré 2 sur } \mathbb{F}_4[x, \theta] \\
 x^4 + x^2 + 1 & : \text{ 5 facteurs à droite de degré 2 sur } \mathbb{F}_4[x, \theta]
 \end{array}$$

4 codes  $\theta$ -centraux non équivalents

$(x^2 + 1)/(x^4 - 1)$	cyclique
$(x^2 + \alpha^2 x + \alpha)/(x^4 - 1)$	$\theta$ -cyclique
$(x^2 + x + 1)/(x^4 + x^2 + 1)$	$\theta$ -central
$(x^2 + \alpha)/(x^4 + x^2 + 1)$	$\theta$ -central

**Exemple : codes  $\theta$ -centraux  $[4, 2]$  sur  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$  avec  $\theta : a \mapsto a^2$ .**

[BGU]

$$\begin{aligned}
 x^4 - 1 & : 7 \text{ facteurs à droite de degré 2 sur } \mathbb{F}_4[x, \theta] \\
 x^4 + x^2 + 1 & : 5 \text{ facteurs à droite de degré 2 sur } \mathbb{F}_4[x, \theta]
 \end{aligned}$$

4 codes  $\theta$ -centraux non équivalents

$(x^2 + 1)/(x^4 - 1)$	cyclique	4, 2, 2
$(x^2 + \alpha^2 x + \alpha)/(x^4 - 1)$	$\theta$ -cyclique	4, 2, <b>3</b>
$(x^2 + x + 1)/(x^4 + x^2 + 1)$	$\theta$ -central	4, 2, 2
$(x^2 + \alpha)/(x^4 + x^2 + 1)$	$\theta$ -central	4, 2, 2

Meilleures distances de codes  $\theta$ -centraux sur  $\mathbb{F}_4[X, \theta]$ .

[BU]

$n \setminus n - k$	2	3	4	5	6	7	8	9	10
4	$C_{3s}^\theta$	$C_4$							
6	$C_2$	$C_4$	$C_4^\theta$	$C_6$					
8	$C_2$	$C_3^\theta$	$C_{4s}^\theta$	$C_5^\theta$	$C_6^\theta$	$C_8$			
10	$C_2$	$\theta_3$	$C_4^\theta$	$C_5^\theta$	$C_6^\theta$	$\theta_6$	$\theta_8$	$C_{10}$	
12	$C_2$	$\theta_3$	$\theta_4$	$C_4$	$C_{6s}^\theta$	$C_6^\theta$	$C_7^\theta$	$C_8^\theta$	$C_9^\theta$
14	$C_2$	$C_3^\theta$	$C_4^\theta$	$C_4$	$C_5^\theta$	$C_{6s}^\theta$	$C_7^\theta$	-1	-1
16	$C_2$	-1	-1	$C_4^\theta$	-1	-1	-1	-1	$C_8^\theta$
18	$C_2$	-1	$\theta_3$	$\theta_4$	-1	-1	$C_6^\theta$	-1	$C_8^\theta$
20	-1	$\theta_3$	$\theta_3$	$\theta_4$	-1	-1	$\theta_6$	$C_7^\theta$	$C_8^\theta$
22	$\theta_2$	$\theta_2$	$\theta_3$	$\theta_4$	$\theta_4$	$\theta_5$	-1	$C_6^\theta$	$C_7^\theta$
24	$C_2^\theta$	$C_2^\theta$	$\theta_3$	$C_4^\theta$	$C_4^\theta$	-1	-1	$C_6^\theta$	$C_7^\theta$
26	$\theta_2$	$\theta_2$	$\theta_3$	$\theta_4$	$\theta_4$	-1	-1	$C_6^\theta$	-1
28	$C_2^\theta$	$C_2^\theta$	$\theta_3$	$C_4^\theta$	$C_4^\theta$	-1	$\theta_5$	$C_6^\theta$	$C_6^\theta$
30	$C_2^\theta$	$C_2^\theta$	$C_3^\theta$	$C_4^\theta$	$C_4^\theta$	-1	$C_5^\theta$	$C_6^\theta$	$C_6^\theta$
32	$C_2^\theta$	$C_2^\theta$	-1	-1	$\theta_4$	-1	$\theta_5$	$C_6^\theta$	$\theta_6$
34	$\theta_2$	$\theta_2$	-1	-1	$\theta_4$	-1	$C_5^\theta$	$C_6^\theta$	$C_6^\theta$
36	$C_2^\theta$	$C_2^\theta$	-1	-1	$\theta_4$	-1	-1	-1	$\theta_6$
38	$\theta_2$	$\theta_2$	-1	-1	$\theta_4$	-1	-1	-1	$\theta_6$
40	$C_2^\theta$	$C_2^\theta$	-1	-1	$\theta_4$	-1	-1	-1	$\theta_6$
42	$C_2^\theta$	$C_2^\theta$	-1	$C_3^\theta$	$C_4^\theta$	-1	-1	-1	$C_6^\theta$
44	$C_2^\theta$	$C_2^\theta$	-1	$\theta_3$	$\theta_4$	$\theta_4$	-1	-1	-1

**Matrice génératrice.**

$$C(x) = (g(x))/(f(x)), \deg(f) = n, \deg(g) = n - k$$

$$\begin{aligned} C(x) &= \{m(x)g(x), \deg(m(x)) = k - 1\} \\ &= \left\{ \sum_{i=0}^{k-1} m_i x^i g(x), m_i \in \mathbb{F}_q \right\} \end{aligned}$$

$$C = \{mG, m \in \mathbb{F}_q^k\}$$

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & \theta(g_0) & & \cdots & \theta(g_{n-k}) & \cdots & 0 \\ 0 & & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & & & & & & \\ 0 & \cdots & 0 & \theta^{k-1}(g_0) & \cdots & \theta^{k-1}(g_{n-k}) \end{pmatrix}$$

## Définitions.

- Produit scalaire

euclidien sur  $\mathbb{F}_q^n$  :

$$\langle x, y \rangle = \sum x_i y_i \text{ pour } x, y \in \mathbb{F}_q^n.$$

hermitien sur  $\mathbb{F}_q^n$  avec  $q$  puissance paire :

$$\langle x, y \rangle_H = \sum x_i y_i^{\sqrt{q}} \text{ pour } x, y \in \mathbb{F}_q^n$$

- Dual de  $C$  :

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

- $\dim(C^\perp) = n - k$
- $C$  est auto-dual si

$$C = C^\perp$$

Dual d'un code  $\theta$ -cyclique pour le produit scalaire euclidien.

[BU]

Soient

$$C(x) = (g(x))/(x^n - 1) \subset \mathbb{F}_q[x, \theta]/(x^n - 1), \deg(g) = n - k$$

$$x^n - 1 = h(x)g(x) = g(x)h(x)$$

alors

$$C^\perp(x) = (g^\perp(x))/(x^n - 1) \subset \mathbb{F}_q[x, \theta]/(x^n - 1)$$

avec

$$g^\perp(x) = \sum_{i=0}^k \theta^i (h_{k-i}) x^i$$

**Preuve.**

- $g^\perp(x) \mid_r x^n - 1$ .
- Soit  $c \in C$ . Pour  $i \in \{0, \dots, n - k - 1\}$

$$\begin{aligned} \langle c(x), x^i g^\perp(x) \rangle &= \sum_{j=i}^{i+k} c_j \theta^j (h_{k+i-j}) \\ &= \text{terme de degré } k + i \text{ de } c(x)h(x) \\ &= 0 \end{aligned}$$

- $\dim((g^\perp)) = \dim(C^\perp)$

**Exemple sur  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$  avec  $\theta : a \mapsto a^2$ .**

$$x^4 - 1 = (x^2 + \alpha^2 x + \alpha^2)(x^2 + \alpha^2 x + \alpha)$$

$$C(x) = (x^2 + \alpha^2 x + \alpha)/(x^4 - 1) \subset \mathbb{F}_4[x, \theta]/(x^4 - 1)$$

$$\begin{aligned} g^\perp(x) &= \theta^0(1)x^0 + \theta^1(\alpha^2)x^1 + \theta^2(\alpha^2)x^2 \\ &= 1 + \alpha x + \alpha^2 x^2 \\ &= \alpha^2 (x^2 + \alpha^2 x + \alpha) \end{aligned}$$

$$C^\perp = C$$

Construction sur  $\mathbb{F}_4$  des codes auto-duaux  $\theta$ -cycliques.

$$1. (g) = (g^\perp)$$

$$\Leftrightarrow x^{2k} - 1 = \underbrace{\left( x^k + \sum_{i=0}^{k-1} g_i x^i \right)}_{g(x)} \underbrace{\left( \theta^k (g_0^2) + \sum_{i=1}^k \theta^{k-i} (g_0^2) \theta^{k-i} (g_{k-i}) x^i \right)}_{h(x)}$$

→  $2k + 1$  relations algébriques de degrés  $\leq 4$

$$2. \text{Coefficients de } g : g_i^4 - g_i = 0, i = 0 \dots k - 1$$

→  $k$  relations algébriques de degrés 4

3. Construction de l'idéal  $I$  des  $3k + 1$  relations algébriques en  $k$  inconnues sur  $\mathbb{F}_4$ .

4. Calcul de la variété  $V(I)$  de  $I$  sur  $\mathbb{F}_4$ .

Codes  $\theta$ -cycliques auto-duaux euclidiens sur  $\mathbb{F}_4$  de longueur  $\leq 40$ .

longueur	nbe codes auto-duaux	meilleure dist. $d$	meilleure dis. connue [G0]	nbe codes dis. $d$	nbe classes dis. $d$	temps calcul $V(l)$
4	3	3	3	2	1	0.
6	3	3	3	2	1	0.
8	3	4	4	2	1	0.
10	5	4	4	4	1	0.
12	21	6	6	4	1	0.01
14	11	6	6	2	1	0.
16	3	4	6	2	1	0.03
18	27	6	6	12	2	0.02
20	63	8	8	8	1	0.52
22	33	8	8	10	1	0.04
24	93	7	8	16	2	1.92
26	65	8	8	36	3	0.42
28	279	9	9	32	4	45.06
30	285	10	10	8	1	11.1
32	3	4	10	2	1	45.44
34	289	10	10	96	6	35.1
36	1533	11	10	36	3	40345
38	513	11	11	36	2	761
40	1023	12	12	16	1	8544

Dual d'un code  $\theta$ -cyclique pour le produit scalaire hermitien.

[BU]

$q$  puissance paire,  $\theta : a \mapsto a^{\sqrt{q}}$

Soient

$$C(x) = (g(x))/(x^n - 1) \subset \mathbb{F}_q[x, \theta]/(x^n - 1), \deg(g) = n - k$$

$$x^n - 1 = h(x)g(x) = g(x)h(x)$$

alors

$$C^{\perp H}(x) = (g^H(x))/(x^n - 1) \subset \mathbb{F}_q[x, \theta]/(x^n - 1)$$

$$g^H(x) = \sum_{i=0}^k \theta^{i+1} (h_{k-i}) x^i$$

Codes  $\theta$ -cycliques auto-duaux hermitiens sur  $\mathbb{F}_4$  de longueur  $\leq 40$ .

longueur	nbe codes auto-duaux	meilleure dist. $d$	meilleure dist. connue [G0]	nbe codes dist. $d$	nbe classes dist. $d$	temps calcul $V(I)$
4	1	2	2	1	1	0.
6	9	4	4	6	1	0.
8	1	2	4	1	1	0.
10	15	4	4	12	2	0.
12	7	4	4	6	1	0.
14	33	6	8	18	1	0.02
16	1	2	8	1	1	0.
18	81	6	8	54	3	0.16
20	21	6	8	6	1	0.01
22	99	8	8	60	2	0.75
24	31	6	8	24	2	0.04
26	195	8	8	144	5	7.91
28	93	10	10	48	2	0.39
30	855	12	12	24	1	123.28
32	1	2	10	1	1	0.140
34	867	10	10	486	14	601.5
36	511	10	12	216	6	48.7
38	1539	12	12	216	4	13 416
40	341	10	12	84	3	33.56

## Une première généralisation des codes 'BCH'.

Soient  $\theta : a \mapsto a^2 \in \text{Aut}(\mathbb{F}_{2^n})$ ,

$$C(x) = (g(x))/(x^n - 1) \subset \mathbb{F}_{2^n}[x, \theta]/(x^n - 1).$$

Soit  $\alpha$  tel que  $\mathbb{F}_{2^n} = \mathbb{F}_2(\alpha)$ .

Soit  $\delta \geq 2$ .

Si

$$x - \alpha^i \mid_r g, \quad i \in \{1, \dots, \delta - 1\}$$

alors

$$d \geq \delta$$

## Preuve.

Soit  $c \in \mathcal{C}$  de poids  $\leq \delta - 1$ ,

$$c(x) = \sum_{j \in \mathcal{J}} c_j x^j \text{ avec } \mathcal{J} \subset \{0, \dots, n-1\}, \text{card}(\mathcal{J}) = \delta - 1$$

$$x - \alpha^i \mid_r c(x) \text{ donc } \tilde{c}(\alpha^i) = 0, i = 1, \dots, \delta - 1$$

où

$$\tilde{c}(z) = \sum_{j \in \mathcal{J}} c_j z^{2^j - 1} \in \mathbb{F}_q[z]$$

donc  $H^t c_{\mathcal{J}} = 0$  où  $H_{i,j} = (\alpha^i)^{2^j - 1}$ ,  $i, j \in \{1, \dots, \delta - 1\}$  et

$$\det(H) = \prod_{j \neq l, j, l \in \mathcal{J}} (\alpha^{2^j - 1} - \alpha^{2^l - 1})$$

$\det(H) \neq 0$  donc  $c = 0$  et  $d \geq \delta$ .

## Décodage : polynôme syndrôme.

$$C(x) = (g(x))/(x^n - 1), \quad g(x) = \text{lcm}_{1 \leq i \leq \delta-1} (x - \alpha^i), \quad \delta = 2t + 1$$

canal

$$c(x) \in C(x) \xrightarrow{\text{canal}} c'(x) = c(x) + e(x)$$

$$e(x) = \sum_{j=1}^{r \leq t} e_j x^{tj}$$

$$\text{Polynôme syndrôme : } S_\delta(z) := \sum_{i=1}^{\delta-1} \tilde{c}'(\alpha^i) z^{i-1} \in \mathbb{F}_q[z].$$

$$\boxed{c' \in C \Leftrightarrow S_\delta(z) = 0}$$

## Décodage : équation clé.

$$S(z) := \sum_{i=1}^{\infty} \check{e}(\alpha^i) z^{i-1} \in \mathbb{F}_q[z].$$

$$S(z) = \frac{w(z)}{\sigma(z)}$$

$$\sigma(z) := \prod_{j=1}^r (1 - \alpha^{\mathcal{I}_j} z) : \text{polynôme pseudo-localisateur}$$

$$w(z) := \sum_{l=1}^r e_l \alpha^{\mathcal{I}_l} \prod_{j \neq l} (1 - \alpha^{\mathcal{I}_j} z) : \text{polynôme évaluateur}$$

avec

$$\mathcal{I}_j = 2^j - 1 : \text{pseudo-positions d'erreurs}$$

## Décodage : équation clé.

- $S(z) = \frac{w(z)}{\sigma(z)}$  (équation clé)
- $S_\delta(z) = S(z) \bmod z^{2t}$
- $\begin{cases} \deg(\sigma) = r \leq t \\ \deg(w) \leq t \\ \text{pgcd}(w(z), \sigma(z)) = 1 \end{cases}$

donc  $\frac{w(z)}{\sigma(z)}$  approximant de Padé  $(t, t)$  pour  $S_\delta(z)$

## Décodage : généralisation de l'algorithme d'Euclide &amp; Sugiyama.

Entrée :  $c', \delta = 2t + 1$

Sortie : mot de code  $c$  tel que  $c' = c + e$  où  $e(x) = \sum_{j=1}^r e_j x^{i_j}$  et  $r \leq t$ .

1. Calculer le polynôme syndrôme  $S_\delta(z)$ .
2. Si  $S_\delta(z) = 0$  retourner  $c = c'$
3. Calculer  $\frac{w(z)}{\sigma(z)}$  : approximant de Padé  $(t, t)$  de  $S_\delta(z)$ .
4. Dédire de  $\sigma(z)$  les pseudo-positions d'erreurs  $\mathcal{I}_1, \dots, \mathcal{I}_r$  et de  $w(z)$  les coefficients d'erreurs :  $e_1, \dots, e_r$
5. Retourner  $c(x) = c'(x) - \sum_{j=1}^r e_j x^{i_j}$  où  $i_j = \log_2(\mathcal{I}_j + 1)$

## Exemple, $n = 10, \delta = 5$ .

Polynôme générateur :

$$g(x) = x^5 + \alpha^{963} x^4 + \alpha^{707} x^3 + \alpha^{664} x^2 + \alpha^{921} x + \alpha^{1011}$$

Mot de code :

$$m(x) = \alpha^{548} x^4 + \alpha^{157} x^3 + \alpha^{646} x^2 + \alpha^{211} x + \alpha^{833}$$

$$c(x) = \alpha^{548} x^9 + \alpha^{523} x^8 + \alpha^{284} x^7 + \alpha^{781} x^6 + \alpha^{120} x^5 + \alpha^{491} x^4 + \alpha^{693} x^3 + \alpha^{984} x^2 + \alpha^{197} x + \alpha^{821}$$

Mot perturbé :

$$e(x) = \alpha^{193} x^7 + \alpha^{139} x^6$$

$$c'(x) = \alpha^{548} x^9 + \alpha^{523} x^8 + \alpha^{118} x^7 + \alpha^{100} x^6 + \alpha^{120} x^5 + \alpha^{491} x^4 + \alpha^{693} x^3 + \alpha^{984} x^2 + \alpha^{197} x + \alpha^{821}$$

Décodage :

- $S_5(z) = \alpha^{975} z^3 + \alpha^{1000} z^2 + \alpha^{115} z + \alpha^{441}$
- $\sigma(z) = \alpha^{190} z^2 + \alpha^{35} z + 1$  et  $w(z) = \alpha^{232} z + \alpha^{441}$
- $l_1 = 127, l_2 = 63$  et  $i_1 = 7, i_2 = 6$ ;  $e_1 = \alpha^{193}, e_2 = \alpha^{139}$ .
- $e(x) = \alpha^{193} x^7 + \alpha^{139} x^6$

## Définition et représentation de $GR(4^m)$ .

Définition :

$$GR(4^m) = \mathbb{Z}_4[y]/(h)$$

avec  $h$  polynôme de degré  $m$  *primitif basique* sur  $\mathbb{Z}_4$  :  $h$  unitaire tel que  $\bar{h}$  primitif sur  $\mathbb{F}_2$ .

$$\xi := y + (h(y))$$

Représentation des éléments :

- représentation additive :  $\alpha_0 + \alpha_1\xi + \cdots + \alpha_{m-1}\xi^{m-1}$  avec  $\alpha_i \in \mathbb{Z}_4$
- représentation 2-adique :  $a + 2b$  avec  $a$  et  $b \in \tau = \{0, 1, \xi, \xi^2, \dots, \xi^{2^m-2}\}$

## Anneau des polynômes tordus sur $GR(4^m)$ et idéaux bilatères.

$\theta: a + 2b \mapsto a^2 + 2b^2$  est automorphisme de  $GR(4^m)$  d'ordre  $m$ .

$GR(4^m)[x, \theta]$  est anneau de polynômes tordus dans lequel :

1. les idéaux ne sont plus **tous** principaux ;
2. on peut diviser à droite par des polynômes **unitaires**.

Les  $f \in \mathbb{Z}_4[x^m]$  **unitaires** engendrent des idéaux bilatères.

Codes  $\theta$ -cycliques, -constacycliques, -principaux sur  $GR(4^m)$ .

Code  $\theta$ -principal sur  $GR(4^m)$  :

$$(g)/(f) \subset GR(4^m)[x, \theta]/(f)$$

avec

- $f \in \mathbb{Z}_4[x^m]$ , unitaire
- $g \in GR(4^m)[x, \theta]$ , unitaire
- $g|_r f$ .

Code  $\theta$ -cyclique :  $f = x^n - 1$ ,  $m|n$ .

Code  $\theta$ -constacyclique :  $f = x^n - c$ ,  $c \in \mathbb{Z}_4$ ,  $m|n$ .

## Applications des codes sur $GR(4^2)$ .

[GNS]

### 1. Codes *auto-duaux euclidiens* sur $GR(4^2)$

→ auto-duaux sur  $\mathbb{Z}_4$

→ réseaux unimodulaires sur  $\mathbb{Z}$

### 2. Codes *auto-duaux hermitiens* sur $GR(4^2)$

→ réseaux 3-modulaires sur  $\mathbb{Z}$ .

Codes duaux des codes  $\theta$ -constacycliques sur  $GR(4^2)$ 

Soit  $C(x) = (g(x))/(x^n - c) \subset GR(4^2)[x, \theta]$  avec  $n$  pair,  $c^2 = 1$

$$h(x)g(x) = g(x)h(x) = x^n - c$$

1. Le dual euclidien de  $C(x)$  est  $C^\perp(x) = (g^\perp(x))/(x^n - c)$

$$g^\perp(x) = \sum_{i=0}^k \theta^i (h_{k-i}) x^i$$

2. Le dual hermitien de  $C(x)$  est  $C^H(x) = (g^H(x))/(x^n - c)$

$$g^H(x) = \sum_{i=0}^k \theta^{i+1} (h_{k-i}) x^i$$

## Applications des codes $\theta$ -constacycliques auto-duaux sur $GR(4^2)$ .

[BSU]

1. Codes  $\theta$ -constacycliques *auto-duaux euclidiens* sur  $GR(4^2)$  de longueur 12

→ nouvelle construction du réseau 'Odd Leech' unique réseau unimodulaire de dimension 24 et norme 3 (T. A. Gulliver, M. Harada, 1997).

2. Codes  $\theta$ -constacycliques *auto-duaux hermitiens* sur  $GR(4^2)$  de longueur 14

→ nouvelle construction du réseau 3-modulaire  $\text{Beis}_{14}$  de dimension 28 (C. Bachoc, 1997).

## Bibliographie

- G- E. M. Gabidulin *Theory of codes with maximum rank distance* Problems of information transmission, 1985
- GO- P. Gaborit, A. Otmani *Tables of Euclidian and Hermitian self-dual codes over  $GF(4)$* , 2002
- GNS- P. Gaborit, A. M. Natividad and P. Solé *Eisenstein Lattices, Galois Rings and Quaternary Codes* International Journal of Number Theory Volume 2 (2006), 289–303.
- BGU- D. Boucher, W. Geiselmann, F. Ulmer, *Skew cyclic codes*. Applied Algebra in Engineering, Communication and Computing 18, 379–389, 2007.
- BU- D. Boucher, F. Ulmer, *Coding with skew polynomial rings*, Prépublication IRMAR 08-07, to appear in *Journal of Symbolic Computation*
- BSU- D. Boucher, P. Solé, F. Ulmer *Skew Constacyclic Codes over Galois Rings*, Prépublication IRMAR, janvier 2008
- CLU- L. Chaussade, P. Loidreau, F. Ulmer *Skew codes of prescribed distance or rank* Prépublication IRMAR, mars 2008