Codes tordus de distance ou de rang prescrits

Pierre Loidreau

CELAr et Université de Rennes
Pierre.Loidreau@m4x.org
travail commun avec L. Chaussade et F. Ulmer

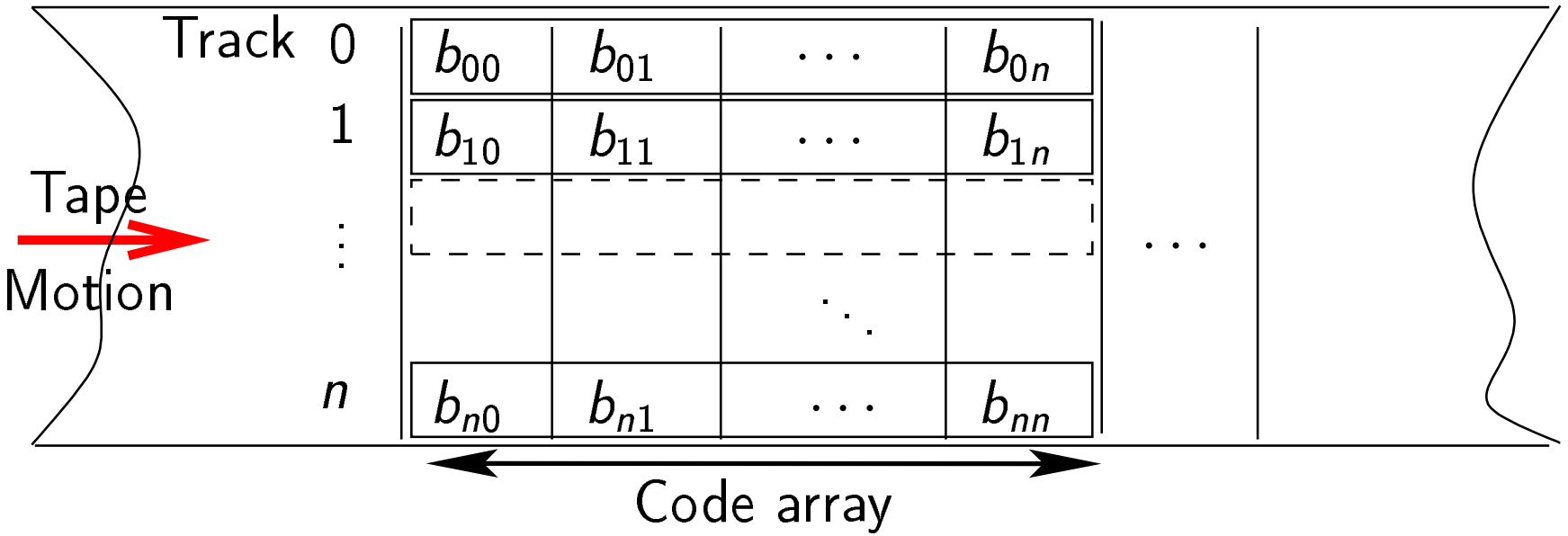
4 juin 2009

Introduction

- Des applications de la métrique rang
- Codes de Gabidulin et polynômes linéaires
- Anneau des polynômes tordus
- Construction de codes tordus
- Perspectives

Des applications de la métrique rang

Correction d'erreurs entrecroisées



- Corriger le long des pistes, [Blaum-McEliece84]
- Théorisation, [Roth91]

Construction de codes Espace-Temps

- Modèle de canal : Canal-ET avec M antennes en transmission et N antennes en réception sur un intervalle T :

$$Y = \rho HS + W, \quad S \in \mathcal{C} \subset \mathcal{A}^{M \times T}$$

- Importance de la diversité $\mathcal{C}$, [Tarokh-Seshadri-Calderbank 98]

$$d = \min_{S_1 \neq S_2 \in \mathcal{C}} \mathrm{Rk}(S_2 - S_1)$$

- Liens entre les codes MRD sur des corps finis et les codes avec un compromis Taux-Diversité optimal, [Lu-Kumar 05]

Codage réseau aléatoire

- Modèle de canal

$$y = Hp + Ge$$

- Recherche de codes de rang constant [Kötter-Kschischang 08]

Historique des applications cryptographiques

- Systèmes de chiffrement, [Gabidulin-Paramonov-Tretjakov 91]
  $\longrightarrow$ Trappe : Difficulté de décoder en métrique rang.
- Codes d'authentification, [Johannson95]
- Schémas d'identification ZK, [Chen96]
- Fonctions de hachage pour MAC, [Savafi-Naini-Charnes 05]

Métrique rang

Definition (Rang d'un vecteur)

- $\gamma_1, \ldots, \gamma_m$, *une base de* $\mathbb{F}_{q^m}/\mathbb{F}_q$,
- $\mathbf{e} = (e_1, \ldots, e_n) \in (\mathbb{F}_{q^m})^n$, $e_i \mapsto (e_{i1}, \ldots, e_{in})$,

$$\forall \mathbf{e} \in \mathbb{F}_{q^m}, \quad \mathrm{Rk}(\mathbf{e}) \stackrel{def}{=} \mathrm{Rk} \begin{pmatrix} e_{11} & \cdots & e_{1n} \\ \vdots & \ddots & \vdots \\ e_{m1} & \cdots & e_{mn} \end{pmatrix}$$

Definition

$\mathcal{C} \subset \mathbb{F}_{q^m}^n$ a un code $(n, M, d)_r$ si

- $M = |\mathcal{C}|$
- *Distance rang min :* $d = \min_{\mathbf{c_1} \neq \mathbf{c_2} \in \mathcal{C}} \mathrm{Rk}(\mathbf{c_1} - \mathbf{c}_2)$

Codes de Gabidulin et polynômes linéaires

Codes de Gabidulin

Soit $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_{q^m}$, où les a_i sont l.i. sur $\mathbb{F}_q$. On considère

$$\mathbf{G} = \begin{pmatrix} a_1 & \cdots & a_n \\ \vdots & \ddots & \vdots \\ a_1^{[k-1]} & \cdots & a_n^{[k-1]} \end{pmatrix}, \text{ where } [i] \stackrel{def}{=} q^i \qquad (1)$$

Definition ([Gabidulin85])

The code engendré par $\mathbf{G}$ *est noté* $Gab_k(\mathbf{a})$.

Propriétés des codes

- Ce sont des codes MRD (ce qui implique MDS ici)
- Le dual de $Gab_k(\mathbf{a})$ est un $Gab_{n-k}(\mathbf{h})$
- La distribution des rangs est connue
- Le groupe des automorphismes semi-linéaires est trivial, [Berger 03]

q-polynômes

Definition ([Øre33])

$$P(z) = \sum_{i=0}^{t} p_i z^{q^i}, \ p_i \in \mathbb{F}_{q^m}$$

If $p_t \neq 0$, $deg_q(P) \stackrel{def}{=} t$ *est le q-degré de* P.

Propriétés

- Anneau non-commutatif muni de $+, \circ$
- Algo. d'Euclide à gauche et à droite
- Algo. d'interpolations et de recherche de racines en temps poly.

Algorithmes de décodage

Algorithme	Complexité (mult. dans $\mathbb{F}_{q^m}$)	
Euclidien ét.	$2t(n+5t)$	[Gabidulin85]
Résolution de syst. lin.	$2t(n+t^2/2)$	[Gabidulin91] [Roth91]
Type BM	$2t(n+3t+t^2/4)$	[Richter-Plass 05]
Type WB	$2t(4n-t)$	[L.05]

Table: Décodage d'erreur de rang $t = \lfloor (d-1)/2 \rfloor$ dans $Gab_{n-d+1}(\mathbf{g})$

Anneau des polyômes tordus – Øre 1933

Construction

- Corps fini $\mathbb{F}_q$
- Automorphisme θ de $\mathbb{F}_q$

$$\mathbb{F}_q[X,\theta] \stackrel{def}{=} \left\{ \sum_{i=0}^{n} p_i X^i,\ n \in \mathbb{N},\ p_i \in \mathbb{F}_q \right\}$$

- " $+$ " : définition usuelle
- " $\cdot$ " : $X \cdot a \stackrel{def}{=} \theta(a)X$

Propriété de l'anneau des polynômes tordus

Proposition

$\mathbb{F}_q[X,\theta]$ est un anneau euclidien à gauche et à droite

- Les idéaux bilatères sont engendrés par

$$X^m \left(\sum_{i=0}^{s} b_i X^{im} \right), \quad b_i \in (\mathbb{F}_q)^\theta,$$

où $m \stackrel{def}{=} |<\theta>|$

- Centre de l'anneau : $Z(\mathbb{F}_q[X,\theta]) = (\mathbb{F}_q)^\theta[X^m]$

Opérateurs de Galois aux différences

- Corps fini $\mathbb{F}_q$
- Automorphisme θ de $\mathbb{F}_q$

$$\mathcal{L}(\mathbb{F}_q) \stackrel{def}{=} \left\{ \sum_{i=0}^{n} p_i \theta^i, \ n \in \mathbb{N}, \ p_i \in \mathbb{F}_q \right\}$$

Morphisme d'anneau entre $(\mathbb{F}_q[X,\theta],+,\cdot)$ et $(\mathcal{L}(\mathbb{F}_q),+,\circ)$ donné pas

$$\sum_{i=0}^{n} p_i X^i \mapsto \sum_{i=0}^{n} p_i \theta^i$$

Clairement surjectif mais pas bijectif

$$\mathcal{L}(\mathbb{F}_q) \sim \mathbb{F}_q[X,\theta]/(X^{|\theta|-1}-1)$$

Lien avec les polynômes linéaires

- Supposons que $q = q_0^t$ et $\theta : y \mapsto y^{q_0}$ alors $(\mathbb{F}_q)^\theta = \mathbb{F}_{q_0}$
- Soit $L = \sum_{i=0}^{n} p_i \theta^i \in \mathcal{L}(\mathbb{F}_q)$
- Soit $\ell = \sum_{i=0}^{n} p_i Y^{[i]} \in \mathbb{F}_q[Y]$, où $[i] = q_0^i$

De manière évidente

$$\forall y \quad L(y) = \ell(y)$$

Definition

ℓ est le q_0-polynôme associé à L

Propriétés des opérateurs de Galois aux différences

- Soit $L = \sum_{i=0}^{n} p_i \theta^i \in \mathcal{L}(\mathbb{F}_q)$

Theorem

Soit $\mathcal{R}_L = \{y \in \overline{\mathbb{F}_q} \mid L(y) = 0\}$ *alors*

- *Chaque élément de* $\mathcal{R}_L$ *est de multiplicité* $k = \min\{i \mid p_i = 0\}$
- *Il existe* s *t.q.* $\mathcal{R}_L \subset \mathbb{F}_{q^s}$
- $\mathcal{R}_L$ *est un e.v. de dimension* $n - k$ *sur* $\mathbb{F}_{q_0}$.

Exemple

- Si $L(y) = \theta^n(y) - y$ alors $\mathcal{R}_L = \mathbb{F}_{q_0^n}$
- Si $L(y) = \theta^n(y) - \theta^{n-1}(y)$ alors $\mathcal{R}_L = \mathbb{F}_{q_0}$

Construction de codes tordus

Codes tordus

Definition ([Boucher-Ulmer 07])

Soir $f \in \mathbb{F}_q[X,\theta]$ de degré n t.q. (f) est bilatère

- *Un idéal à gauche I de $\mathbb{F}_q[X,\theta]/(f)$ est engendré par g t.q. $f = h \cdot g$*

$$(g)/(f) = \{a \cdot g \bmod (f) \mid a \in \mathbb{F}_q[X,\theta]\}$$

est appelé un θ-code

- *Si $m \mid n$ et $f = X^n - 1$, alors $(g)/(f)$ est appelé θ-cylique*

Application

$$\begin{array}{rcl} (g)/(f) & \to & C_\theta(g,f) \\ p = \sum_{i=0}^{n-1} p_i X^i & \mapsto & (p_0,\ldots,p_{n-1}) \end{array}$$

Propriétés

- Matrice génératrice de $C_\theta(g, f)$ si $g = \sum_{i=0}^{r} g_i X^i$:

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

- Si $f = X^n - 1 = h \cdot g$, s.t. $h = \sum_{i=0}^{n-r} h_i X^i$, alors le dual de $(g)/(f)$ est engendré par

$$g^\perp = \sum_{i=0}^{n-r} \theta^{n-i}(h_{n-i}) X^i$$

Borne d'un polynôme

Definition (Borne d'un polynôme)

Soit $f \in \mathbb{F}_q[X, \theta]$. Soit $(f) \subset I$, I le plus petit idéal bilatère. Alors $I = (f^*)$ où f^* est la borne de f.

- Plus petit θ-code engendré par g : $(g)/(g^*)$, où g^* est la borne de g.
- Degré maximal de la borne de f : $\leq mtn$ où
  - m : ordre de θ
  - t : degré de f
  - n : $[\mathbb{F}_q : \mathbb{F}_{q_0}]$

Codes tordus de rang construit (I)

Proposition

Soit $g \in \mathbb{F}_q[X, \theta]$. *Soit* $\beta \in \mathbb{F}_{q^s}$ *et* $m \geq n \geq \delta \geq 1$ *t.q.*

- $\beta, \ldots, \theta^{n-1}(\beta)$ *sont* $\mathbb{F}_{q_0}$*-l.i.*
- $\forall\ i \in \{0, \ldots, \delta - 1\}$, $L_g(\theta^i(\beta)) = 0$

Alors $\forall f \in \mathbb{F}_{q_0}[X^m]$ *t.q.* $f = h \cdot g$ *on a*

$$(g)/(f) \text{ has minimum rank distance } \geq \delta + 1.$$

Ebauche de preuve (I)

- $(c_0, \ldots, c_{n-1})$ de rang t sur $\mathbb{F}_{q_0}$ si et ssi

$$(c_0, \ldots, c_{n-1}) = (C_1, \ldots, C_t)U, \begin{cases} C_1, \ldots, C_t, \text{l.i.} \\ U \in \mathcal{M}_{tn}(\mathbb{F}_{q_0}) \end{cases}$$

- $\mathcal{R}_{L_g} =< \{\beta, \ldots, \theta^{\delta-1}(\beta), \gamma_\delta, \ldots, \gamma_{k-1})\} >$
- Comme $c \in (g)/(f) = a \cdot g$ on a $c(\mathcal{R}_{L_g}) = 0$, c'est-à-dire

$$c \begin{pmatrix} \beta & \cdots & \theta^{\delta-1}(\beta) & \gamma_\delta & \cdots & \gamma_{k-1} \\ \theta(\beta) & \cdots & \theta^{\delta}(\beta) & \theta(\gamma_\delta) & \cdots & \theta(\gamma_{k-1}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ \theta^{n-1}(\beta) & \cdots & \theta^{n+\delta-2}(\beta) & \theta^{n-1}(\gamma_\delta) & \cdots & \theta^{n-1}(\gamma_{k-1}) \end{pmatrix} = 0$$

Ebauche de preuve (II)

- Pour tout $c \in (g)/(f)$ de rang t

$$(C_1, \ldots, C_t) \begin{pmatrix} u_1(\beta) & \cdots & \theta^{\delta-1}(u_1(\beta)) & u_1(\gamma_\delta) & \ldots & u_1(\gamma_{k-1}) \\ u_2(\beta) & \cdots & \theta^{\delta-1}(u_2(\beta)) & u_2(\gamma_\delta) & \ldots & u_2(\gamma_{k-1}) \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ u_t(\beta) & \cdots & \theta^{\delta-1}(u_t(\beta)) & u_t(\gamma_\delta) & \ldots & u_t(\gamma_{k-1}) \end{pmatrix} = 0$$

où $u_i(\beta) = \sum_{j=0}^{n} U_{ij}\theta^i(\beta)$, $U_{ij} \in \mathbb{F}_{q_0}$

- Si $t \leq \delta - 1$, pas de solutions excepté le vecteur 0

Construction de codes tordus de rang prescrit (I)

Trouver des codes tordus de rang δ sur $\mathbb{F}_q$

1. Soit $\theta \in Aut(\mathbb{F}_q) : \rightarrow q_0$ et $F_q[X, \theta]$
2. Prendre β dans une extension $\mathbb{F}_{q^s}$, s entier
3. Trouver le plus grand τ t.q. $\{\beta, \ldots, \theta^{\tau-1}(\beta)\}$ est l.i. sur $\mathbb{F}_{q_0}$
4. Construire $g \in \mathbb{F}_q[X, \theta]$, s.t.

$$L_g(\theta^i(\beta)) = 0, \ \forall i = 0, \ldots, \delta - 1$$

Pas toujours possible

5. Trouver la borne f de g
6. Retourner $C_\theta(g, f)$

Espaces vectoriels et operateurs de Galois aux différences

- Quand l'étape (4) est-elle possible ?

Hypothèses

- Soit $y_1, \ldots, y_n \in \mathbb{F}_{q^s}$ l.i. sur $\mathbb{F}_{q_0}$
- Soit σ generateur de $Aut(\mathbb{F}_{q^s}/\mathbb{F}_q)$
- Soir

$$\mathrm{Cas}(y) \stackrel{def}{=} \begin{vmatrix} y_1 & y_2 & \ldots & y_n & y \\ \theta(y_1) & \theta(y_2) & \ldots & \theta(y_n) & \theta(y) \\ \theta^2(y_1) & \theta^2(y_2) & \ldots & \theta^2(y_n) & \theta^2(y) \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \theta^n(y_1) & \theta^n(y_2) & \ldots & \theta^n(y_n) & \theta^n(y) \end{vmatrix}$$

Casoratien et longueur des codes

Proposition (Casoratien)

- $Cas(y_1, \ldots, y_n, y) = \theta^n + \sum_{i=0}^{n-1} \lambda_i \theta^i \in \mathcal{L}(\mathbb{F}_{q^s})$
- $Cas(y_1, \ldots, y_n, y) = 0 \Leftrightarrow y \in < y_1, \ldots, y_n >$
- $Cas(y_1, \ldots, y_n, y) \in \mathcal{L}(\mathbb{F}_q)$ *ssi* $< y_1, \ldots, y_n >$ *est stable sous l'action de* σ

Lemma (Longueur du code)

Soit $\beta, \ldots, \theta^{\tau-1}(\beta)$ *la plus longue suite l.i. sur* $\mathbb{F}_{q_0}$. *Soit* g *associé à* $Cas(\beta, \ldots, \theta^{\delta-1}(\beta), y)$. *Alors* g^* *est de degré* τ *et*

$$\mathcal{R}_{L_{g^*}} =< \beta, \ldots, \theta^{\tau-1}(\beta) >$$

Construction de codes tordus de rang prescrit (II)

1. Soit $\theta \in Aut(\mathbb{F}_q) : \rightarrow \ q_0$ et $F_q[X, \theta]$
2. Prendre β dans $\mathbb{F}_{q^s}$, $s \leq N$ t.q. $\sigma \in < \theta >$
3. Trouver le plus grand n t.q. $\{\beta, \ldots, \theta^{n-1}(\beta)\}$ est l.i. sur $\mathbb{F}_{q_0}$
4. Soit $L_f(y) = \text{Cas}(\beta, \ldots, \theta^{n-1}(\beta), y)$. On a $f \in \mathbb{F}_{q_0}[X^m]$
5. Construire V_j, le plus petit e.v. sur $\mathbb{F}_{q_0}$ stable sous σ et contenant $\beta, \ldots, \theta^{\delta-1}(\beta)$
6. Construire $g \in \mathbb{F}_q[X, \theta]$, t.q.

$$L_g(V_j) = 0$$

	$\delta = 1$	$\delta = 2$	$\delta = 3$
$\mathbb{F}_{16}$	$[\mathbf{4,3,2}]_g(8)$	$[\mathbf{4,2,3}]_g(8)$	$[\mathbf{4,1,4}]_g(8)$
$\mathbb{F}_{16^2}$	$[\mathbf{8,6,3}]_g(64)$	$[8,4,4]_g(32)$ $[\mathbf{8,4,5}]_g(32)$	$[\mathbf{8,2,7}]_g(64)$
$\mathbb{F}_{16^3}$	$[12,9,2]_g(32)$ $[12,9,3]_g(408)$ $[\mathbf{12,9,4}]_g(72)$ $[\mathbf{8,6,3}](48)$	$[12,6,3]_g(8)$ $[12,6,4]_g(72)$ $[12,6,5]_g(136)$ $[8,4,3](16)$ $[\mathbf{8,4,5}](8)$	$[12,3,4]_g(8)$ $[12,3,6]_g(64)$ $[12,3,8]_g(152)$ $[\mathbf{12,3,10}]_g(72)$ $[8,2,5](8)$ $[\mathbf{8,2,7}](48)$
$\mathbb{F}_{16^4}$	$[16,12,3]_g(256)$ $[16,12,4]_g(3840)$ $[\mathbf{12,9,3}](512)$	$[16,8,6]_g(368)$ $[16,8,7]_g(3008)$ $[\mathbf{16,8,8}]_g(720)$ $[12,6,5](192)$ $[\mathbf{12,6,6}](320)$	$[16,4,10]_g(256)$ $[16,4,11]_g(1536)$ $[\mathbf{16,4,12}]_g(2304)$ $[\mathbf{12,3,8}](512)$

Codes tordus de distance construite

Definition (Codes BCH tordus)

Un code BCH tordu (n, q_0, t, s, δ) *est un* θ*-code engendré par* $g \in \mathbb{F}_{q=q_0^t}[X, \theta]$ *t.q.*

- g *est divisible à droite par* $X - \alpha^k$, $\forall k = 1, \ldots, \delta - 1$, *où* $< \alpha >= \mathbb{F}_{q_0^s}^*$
- g *est borné par* f *de degré* n

Proposition

Si $n \leq (q_0 - 1)s$ *alors sa distance minimum est au moins* δ

Comment les construire ?

- Soit $< \alpha >= \mathbb{F}_{q_0^s}^*$, $\forall i = 1, \ldots, \delta - 1$ calculer β_i, t.q.

$$\theta(\beta_i)/\beta_i = \alpha^i$$

- Construire V_j, le plus petit e.v. sur $\mathbb{F}_{q_0}$ stable sous σ et contenant $\beta_1, \ldots, \beta_{\delta-1}$
- Construire $g \in \mathbb{F}_q[X, \theta]$, t.q.

$$L_g(V_j) = 0,$$

- Calculer $f = g^*$ de degré n

Si $n \leq (q_0 - 1)s$ alors as distance minimale est au moins δ

	$\delta = 2$	$\delta = 3$	$\delta = 4$	$\delta = 5$
$\mathbb{F}_{8^2}$	$[\mathbf{6},\mathbf{4},\mathbf{3}](18)$	$[\mathbf{6},\mathbf{2},\mathbf{5}](12)$ $[\mathbf{6},\mathbf{3},\mathbf{4}](3)$	$[\mathbf{6},\mathbf{2},\mathbf{5}](9)$ $[\mathbf{6},\mathbf{1},\mathbf{6}](3)$	$[\mathbf{6},\mathbf{1},\mathbf{6}](3)$
$\mathbb{F}_{8^3}$	$[9,6,3](108)$ $[\mathbf{9},\mathbf{6},\mathbf{4}](18)$ $[\mathbf{6},\mathbf{3},\mathbf{4}](18)$	$[9,3,6](60)$ $[\mathbf{9},\mathbf{3},\mathbf{7}](12)$ $[9,4,5](12)$ $[\mathbf{9},\mathbf{4},\mathbf{6}](3)$ $[\mathbf{6},\mathbf{2},\mathbf{5}](18)$	$[\mathbf{9},\mathbf{1},\mathbf{9}](6)$ $[9,2,6](6)$ $[\mathbf{9},\mathbf{2},\mathbf{8}](6)$ $[9,3,6](24)$ $[\mathbf{9},\mathbf{3},\mathbf{7}](3)$ $[\mathbf{9},\mathbf{4},\mathbf{5}](3)$	$[\mathbf{9},\mathbf{1},\mathbf{9}](3)$ $[\mathbf{9},\mathbf{2},\mathbf{6}](6)$
$\mathbb{F}_{8^4}$	$[12,8,3](132)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](183)$ $[\mathbf{9},\mathbf{6},\mathbf{3}](54)$	$[12,4,5](12)$ $[12,4,6](60)$ $[\mathbf{12},\mathbf{4},\mathbf{7}](48)$ $[12,5,6](21)$ $[\mathbf{12},\mathbf{5},\mathbf{7}](12)$ $[\mathbf{12},\mathbf{7},\mathbf{4}](3)$ $[\mathbf{12},\mathbf{8},\mathbf{4}](72)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](6)$ $[12,2,6](3)$ $[12,2,8](6)$ $[\mathbf{12},\mathbf{2},\mathbf{10}](9)$ $[12,3,6](6)$ $[\mathbf{12},\mathbf{3},\mathbf{9}](18)$ $[12,4,7](9)$	$[\mathbf{12},\mathbf{1},\mathbf{12}](3)$ $[12,2,6](3)$ $[12,2,8](6)$ $[\mathbf{12},\mathbf{2},\mathbf{10}](3)$ $[12,3,6](9)$ $[\mathbf{12},\mathbf{3},\mathbf{9}](3)$ $[12,4,6](3)$

Résultats obtenus

- Avec la méthode du rang : $[42, 14, 21]_8$, borne de Griesmer : 25
- Avec la méthode BCH : $[40, 23, 10]_4$, borne de Griesmer : 13

Perspectives et questions ouvertes

- Recherche de nouveau codes avec de bons paramètres
- Applications cryptographiques
- Applications des codes de rang prescrit en théorie des codes correcteurs