Codes tordus dont le rang ou la distance minimale est prescrite

Lionel Chaussade, Pierre Loidreau, Félix Ulmer

IRMAR, UMR 6625, Université de Rennes 1

Luminy, Octobre 2008

Plan

Plan

Plan

Plan

Notations et construction

$$\begin{array}{ccccccc}
Id & & \mathbb{F}_{q^s} & & & & \\
\cap & & \cup & & & & \\
\sigma(x) = x^q & \leftrightsquigarrow & \mathbb{F}_q & = & (\mathbb{F}_{q^s})^\sigma & \leftrightsquigarrow & Id \\
\cap & & \cup & & & & \cap \\
\Theta(x) = x^{q_0} & \leftrightsquigarrow & \mathbb{F}_{q_0} & = & (\mathbb{F}_q)^\theta & \leftrightsquigarrow & \theta(x) = x^{q_0}
\end{array}$$

Notations et construction

$$
\begin{array}{ccccccc}
Id & \rightsquigarrow & \mathbb{F}_{q^s} & & & & \\
\cap & & \cup & & & & \\
\sigma(x) = x^q & \rightsquigarrow & \mathbb{F}_q & = & (\mathbb{F}_{q^s})^{\sigma} & \rightsquigarrow & Id \\
\cap & & \cup & & & & \cap \\
\Theta(x) = x^{q_0} & \rightsquigarrow & \mathbb{F}_{q_0} & = & (\mathbb{F}_q)^{\theta} & \rightsquigarrow & \theta(x) = x^{q_0}
\end{array}
$$

Notations et construction

$$
\begin{array}{ccccccc}
Id & \rightsquigarrow & \mathbb{F}_{q^s} & & & & \\
\cap & & \cup & & & & \\
\sigma(x) = x^q & \rightsquigarrow & \mathbb{F}_q & = & (\mathbb{F}_{q^s})^{\sigma} & \rightsquigarrow & Id \\
\cap & & \cup & & & & \cap \\
\Theta(x) = x^{q_0} & \rightsquigarrow & \mathbb{F}_{q_0} & = & (\mathbb{F}_q)^{\theta} & \rightsquigarrow & \theta(x) = x^{q_0}
\end{array}
$$

Notations et construction

$$
\begin{array}{ccccccc}
Id & \rightsquigarrow & \mathbb{F}_{q^s} & & & & \\
\cap & & \cup & & & & \\
\sigma(x) = x^q & \rightsquigarrow & \mathbb{F}_q & = & (\mathbb{F}_{q^s})^{\sigma} & \rightsquigarrow & Id \\
\cap & & \cup & & & & \cap \\
\Theta(x) = x^{q_0} & \rightsquigarrow & \mathbb{F}_{q_0} & = & (\mathbb{F}_q)^{\theta} & \rightsquigarrow & \theta(x) = x^{q_0}
\end{array}
$$

Notations et construction

$$
\begin{array}{ccccccc}
Id & \rightsquigarrow & \mathbb{F}_{q^s} & & & & \\
\cap & & \cup & & & & \\
\sigma(x) = x^q & \rightsquigarrow & \mathbb{F}_q & = & (\mathbb{F}_{q^s})^{\sigma} & \rightsquigarrow & Id \\
\cap & & \cup & & & & \cap \\
\Theta(x) = x^{q_0} & \rightsquigarrow & \mathbb{F}_{q_0} & = & (\mathbb{F}_q)^{\theta} & \rightsquigarrow & \theta(x) = x^{q_0}
\end{array}
$$

Notations et construction

$$
\begin{array}{ccccccc}
Id & & \mathbb{F}_{q^s} & & & & \\
\cap & & \cup & & & & \\
\sigma(x) = x^q & \leftrightsquigarrow & \mathbb{F}_q & = & (\mathbb{F}_{q^s})^{\sigma} & \leftrightsquigarrow & Id \\
\cap & & \cup & & & & \cap \\
\Theta(x) = x^{q_0} & \leftrightsquigarrow & \mathbb{F}_{q_0} & = & (\mathbb{F}_q)^{\theta} & \leftrightsquigarrow & \theta(x) = x^{q_0}
\end{array}
$$

L'anneau $\mathbb{F}_q[X, \theta]$

Soit θ un automorphisme de $\mathbb{F}_q$:

$$\mathbb{F}_q[X, \theta] = \{a_0 + ... + a_n X^n, \ a_i \in \mathbb{F}_q\}$$

Règle de multiplication :

$$\boxed{Xa = \theta(a)X}$$

Théorème

L'anneau $\mathbb{F}_q[X, \theta]$ est euclidien à droite et à gauche. En particulier les idéaux sont principaux.

Codes θ-cycliques

Commutatif	Tordu
$g \in \mathbb{F}_q[X]$	$g \in \mathbb{F}_q[X, \theta]$
$g \mid X^n - 1$	$g \mid_d X^n - 1$
(g) idéal de $\mathbb{F}_q[X]/(X^n - 1)$	(g) idéal de $\mathbb{F}_q[X, \theta]/(X^n - 1)$
Code cyclique	Code θ-cyclique

θ-codes

Définition

Un θ-code est un idéal à gauche de $\mathbb{F}_q[X,\theta]/(f)$ où (f) est bilatère.

$$g = g_0 + g_1 X + \ldots + g_r X^r \in \mathbb{F}_q[X,\theta]$$

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

θ-codes

Définition

Un θ-code est un idéal à gauche de $\mathbb{F}_q[X,\theta]/(f)$ où (f) est bilatère.

$$g = g_0 + g_1 X + ... + g_r X^r \in \mathbb{F}_q[X,\theta]$$

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

θ-codes

Définition

Un θ-code est un idéal à gauche de $\mathbb{F}_q[X,\theta]/(f)$ où (f) est bilatère.

$$g = g_0 + g_1 X + \ldots + g_r X^r \in \mathbb{F}_q[X,\theta]$$

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

Question : Peut-on contrôler la distance minimale de ces codes?

Equations aux différences

Définition

Une équation aux différences sur $\mathbb{F}_q$ est :

$$L(y) = a_n\theta^n(y) + ... + a_1\theta(y) + a_0 y = 0$$

où $a_i \in \mathbb{F}_q$ et θ un automorphisme de $\mathbb{F}_q$.
L'ensemble des solutions est un $(\mathbb{F}_q)^\theta$-espace vectoriel.

$$L(y) = \sum_{k=0}^{n} y^{p^{ki}} \text{ si } \theta(y) = y^{p^i}$$

$\Rightarrow$ Polynômes linéarisés

Equations aux différences

Définition

Une équation aux différences sur $\mathbb{F}_q$ est :

$$L(y) = a_n\theta^n(y) + \ldots + a_1\theta(y) + a_0 y = 0$$

où $a_i \in \mathbb{F}_q$ et θ un automorphisme de $\mathbb{F}_q$.
L'ensemble des solutions est un $(\mathbb{F}_q)^\theta$-espace vectoriel.

$$L(y) = \sum_{k=0}^{n} y^{p^{ki}} \text{ si } \theta(y) = y^{p^i}$$

$\Rightarrow$ Polynômes linéarisés

Equations aux différences

Définition

Une équation aux différences sur $\mathbb{F}_q$ est :

$$L(y) = a_n\theta^n(y) + \ldots + a_1\theta(y) + a_0 y = 0$$

où $a_i \in \mathbb{F}_q$ et θ un automorphisme de $\mathbb{F}_q$.
L'ensemble des solutions est un $(\mathbb{F}_q)^\theta$-espace vectoriel.

$$L(y) = \sum_{k=0}^{n} y^{p^{ki}} \text{ si } \theta(y) = y^{p^i}$$

$\Rightarrow$ Polynômes linéarisés

Lien avec les polynômes tordus

$$L(y) = a_n\theta^n(y) + \ldots + a_0 y \quad \rightsquigarrow \quad P_L = a_n X^n + \ldots + a_0 \text{ (skew)}$$

$$L_1 \circ L_2 \quad \rightsquigarrow \quad P_{L_1} P_{L_2}$$

$$\beta \in \mathbb{F}_{q^s}^*,\ L(\beta) = 0 \quad \rightsquigarrow \quad (X - \frac{\theta(\beta)}{\beta}) \mid_d P_L$$

Lien avec les polynômes tordus

$$L(y) = a_n\theta^n(y) + \ldots + a_0 y \quad \rightsquigarrow \quad P_L = a_n X^n + \ldots + a_0 \text{ (skew)}$$

$$L_1 \circ L_2 \quad \rightsquigarrow \quad P_{L_1} P_{L_2}$$

$$\beta \in \mathbb{F}_{q^s}^*,\ L(\beta) = 0 \quad \rightsquigarrow \quad (X - \tfrac{\theta(\beta)}{\beta}) \mid_d P_L$$

Lien avec les polynômes tordus

$$L(y) = a_n\theta^n(y) + \ldots + a_0 y \quad \leftrightsquigarrow \quad P_L = a_n X^n + \ldots + a_0 \text{ (skew)}$$

$$L_1 \circ L_2 \quad \leftrightsquigarrow \quad P_{L_1} P_{L_2}$$

$$\beta \in \mathbb{F}_{q^s}^*,\ L(\beta) = 0 \quad \leftrightsquigarrow \quad (X - \frac{\theta(\beta)}{\beta}) \mid_d P_L$$

Distance rang

On fixe une base $(\beta_1, ..., \beta_m)$ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.

Definition

Soit $x = (x_1, ..., x_n) \in (\mathbb{F}_{q^m})^n$, on appelle rang de x, le rang de la matrice $X = (x_{ij})$ où $x_j = \sum_{i=1}^{m} x_{ij}\beta_j$.

Definition

La distance rang minimale d'un code $C \subset (\mathbb{F}_{q^m})^n$ est :

$$d_{\text{rang}}(C) = \min_{x \in C^*} \text{rang}(x)$$

$$d_{\text{rang}}(C) \leq d_{\text{hamming}}(C)$$

Distance rang

On fixe une base $(\beta_1, ..., \beta_m)$ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.

Definition

Soit $x = (x_1, ..., x_n) \in (\mathbb{F}_{q^m})^n$, on appelle rang de x, le rang de la matrice $X = (x_{ij})$ où $x_j = \sum_{i=1}^{m} x_{ij}\beta_j$.

Definition

La distance rang minimale d'un code $C \subset (\mathbb{F}_{q^m})^n$ est :

$$d_{\text{rang}}(C) = \min_{x \in C^*} \text{rang}(x)$$

$$d_{\text{rang}}(C) \leq d_{\text{hamming}}(C)$$

Distance rang

On fixe une base $(\beta_1, ..., \beta_m)$ de $\mathbb{F}_{q^m}$ sur $\mathbb{F}_q$.

Definition

Soit $x = (x_1, ..., x_n) \in (\mathbb{F}_{q^m})^n$, on appelle rang de x, le rang de la matrice $X = (x_{ij})$ où $x_j = \sum_{i=1}^{m} x_{ij}\beta_j$.

Definition

La distance rang minimale d'un code $C \subset (\mathbb{F}_{q^m})^n$ est :

$$d_{\text{rang}}(C) = \min_{x \in C^*} \text{rang}(x)$$

$$\boxed{d_{\text{rang}}(C) \leq d_{\text{hamming}}(C)}$$

Prescription de la distance rang

Théorème

Soit $g \in \mathbb{F}_q[X, \theta]$ et L_g l'opérateur associé. Soit $\beta \in \mathbb{F}_{q^s}$ et $\delta \geq 1$ tels que :

-$\beta, \ldots, \theta^{n-1}(\beta)$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$.

-$\beta, \ldots, \theta^{\delta-1}(\beta)$ des solutions de $L_g(y) = 0$.

Alors pour tout f central de degré au plus n, le code $(g)/(f)$ a une distance rang au moins égale à $\delta + 1$.

Prescription de la distance rang

Théorème

Soit $g \in \mathbb{F}_q[X, \theta]$ et L_g l'opérateur associé. Soit $\beta \in \mathbb{F}_{q^s}$ et $\delta \geq 1$ tels que :

-β,...,$\theta^{n-1}(\beta)$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$.

-β,...,$\theta^{\delta-1}(\beta)$ des solutions de $L_g(y) = 0$.

Alors pour tout f central de degré au plus n, le code $(g)/(f)$ a une distance rang au moins égale à $\delta + 1$.

Prescription de la distance rang

Théorème

Soit $g \in \mathbb{F}_q[X, \theta]$ et L_g l'opérateur associé. Soit $\beta \in \mathbb{F}_{q^s}$ et $\delta \geq 1$ tels que :

-β,...,$\theta^{n-1}(\beta)$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$.

-β,...,$\theta^{\delta-1}(\beta)$ des solutions de $L_g(y) = 0$.

Alors pour tout f central de degré au plus n, le code $(g)/(f)$ a une distance rang au moins égale à $\delta + 1$.

Prescription de la distance rang

Théorème

Soit $g \in \mathbb{F}_q[X, \theta]$ et L_g l'opérateur associé. Soit $\beta \in \mathbb{F}_{q^s}$ et $\delta \geq 1$ tels que :
-β,...,$\theta^{n-1}(\beta)$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$.
-β,...,$\theta^{\delta-1}(\beta)$ des solutions de $L_g(y) = 0$.
Alors pour tout f central de degré au plus n, le code $(g)/(f)$ a une distance rang au moins égale à $\delta + 1$.

Algorithme

1. Choisir $\mathbb{F}_q$, $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, s et δ.
2. Prendre $\beta \in \mathbb{F}_{q^s}$ et calculer le plus grand n tel que

   $$\beta, ..., \theta^{n-1}(\beta) \text{ soient linéairement indépendants sur } (\mathbb{F}_q)^\theta.$$

3. On veut trouver un opérateur ayant pour solutions $\beta, ..., \theta^{\delta-1}(\beta)$.

Algorithme

1. Choisir $\mathbb{F}_q$, $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, s et δ.
2. Prendre $\beta \in \mathbb{F}_{q^s}$ et calculer le plus grand n tel que

   $\beta, ..., \theta^{n-1}(\beta)$ soient linéairement indépendants sur $(\mathbb{F}_q)^\theta$.

3. On veut trouver un opérateur ayant pour solutions $\beta, ..., \theta^{\delta-1}(\beta)$.

Algorithme

1. Choisir $\mathbb{F}_q$, $\theta \in \mathrm{Aut}(\mathbb{F}_q)$, s et δ.
2. Prendre $\beta \in \mathbb{F}_{q^s}$ et calculer le plus grand n tel que

   $$\beta, ..., \theta^{n-1}(\beta) \text{ soient linéairement indépendants sur } (\mathbb{F}_q)^\theta.$$

3. On veut trouver un opérateur ayant pour solutions $\beta, ..., \theta^{\delta-1}(\beta)$.

Casoratien

Soient $y_1, ..., y_n \in \mathbb{F}_{q^s}$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$:

$$Cas_{y_1,...,y_n}(y) = \begin{vmatrix} y_1 & y_2 & \dots & y_n & y \\ \theta(y_1) & \theta(y_2) & \dots & \theta(y_n) & \theta(y) \\ \theta^2(y_1) & \theta^2(y_2) & \dots & \theta^2(y_n) & \theta^2(y) \\ \dots & \dots & \dots & \dots & \dots \\ \theta^n(y_1) & \theta^n(y_2) & \dots & \theta^n(y_n) & \theta^n(y) \end{vmatrix}$$

$$\Rightarrow L_g = Cas(\beta, ..., \theta^{\delta-1}(\beta), \gamma_1, ..., \gamma_r)$$

Casoratien

Soient $y_1, ..., y_n \in \mathbb{F}_{q^s}$ linéairement indépendants sur $(\mathbb{F}_q)^\theta$:

$$Cas_{y_1,...,y_n}(y) = \begin{vmatrix} y_1 & y_2 & \dots & y_n & y \\ \theta(y_1) & \theta(y_2) & \dots & \theta(y_n) & \theta(y) \\ \theta^2(y_1) & \theta^2(y_2) & \dots & \theta^2(y_n) & \theta^2(y) \\ \dots & \dots & \dots & \dots & \dots \\ \theta^n(y_1) & \theta^n(y_2) & \dots & \theta^n(y_n) & \theta^n(y) \end{vmatrix}$$

$$\Rightarrow L_g = Cas(\beta, ..., \theta^{\delta-1}(\beta), \gamma_1, ..., \gamma_r)$$

Stabilité et corps de définition

Théorème

Le $(\mathbb{F}_q)^\theta$- espace vectoriel engendré par $y_1, ..., y_n$ est stable par $\sigma(x) = x^q$ si et seulement si $Cas(y_1, ..., y_n)$ est à coefficients dans $\mathbb{F}_q$.

Cacul de la borne

Proposition

On suppose que σ est une puissance de θ. Le degré de la borne, f, de g est plus petit que n si et seulement si $L_f = Cas(\beta, ..., \theta^{n-1}(\beta))$.

Algorithme final

1. Choisir $\mathbb{F}_q$, $\theta \in Aut(\mathbb{F}_q)$, s et δ.
2. Prendre $\beta \in \mathbb{F}_{q^s}$ et calculer le plus grand n tel que

   $$\beta, ..., \theta^{n-1}(\beta) \text{ soient linéairement indépendants sur } (\mathbb{F}_q)^\theta.$$

3. Calculer le casoratien de ces éléments. S'il est central, on continue, sinon on choisit un autre β.
4. Compléter la famille $\beta, ..., \theta^{\delta-1}(\beta)$ pour former un sous-$(\mathbb{F}_q)^\theta$-espace vectoriel V stable par σ.
5. Calculer $L_g = Cas(V)$.
6. Former le θ code correspondant.

On a un θ-code de distance rang $\geq \delta + 1$

Un exemple détaillé

1. $\mathbb{F}_4$, $\theta(x) = x^2$, $s = 6$ et $\sigma(x) = x^4$.
2. $\beta = \alpha^{3688}$. La famille $\beta, ..., \theta^7(\beta)$ est linéairement indépendante sur $\mathbb{F}_2$.
3. Le casoratien de ces éléments est $L_f = X^8 + X^6 + X^2 + 1$ qui est central.
4. On prend $\delta = 1$ et on forme le plus petit espace stable par $\sigma(x) = x^4$ contenant β. Le casoratien d'une base de cet espace est : $L_g = X^4 + w^2X^3 + X^2 + X + 1$.
5. On obtient un code sur $\mathbb{F}_4$ qui a pour matrice génératrice :
$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$
6. $[8, 4, 4]$ code, c'est un θ-code. Il descend en un [16,8,4] code sur $\mathbb{F}_2$.

Un exemple détaillé

1. $\mathbb{F}_4$, $\theta(x) = x^2$, $s = 6$ et $\sigma(x) = x^4$.
2. $\beta = \alpha^{3688}$. La famille $\beta, ..., \theta^7(\beta)$ est linéairement indépendante sur $\mathbb{F}_2$.
3. Le casoratien de ces éléments est $L_f = X^8 + X^6 + X^2 + 1$ qui est central.
4. On prend $\delta = 1$ et on forme le plus petit espace stable par $\sigma(x) = x^4$ contenant β. Le casoratien d'une base de cet espace est : $L_g = X^4 + w^2X^3 + X^2 + X + 1$.
5. On obtient un code sur $\mathbb{F}_4$ qui a pour matrice génératrice :
$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$
6. $[8, 4, 4]$ code, c'est un θ-code. Il descend en un [16,8,4] code sur $\mathbb{F}_2$.

Un exemple détaillé

1. $\mathbb{F}_4$, $\theta(x) = x^2$, $s = 6$ et $\sigma(x) = x^4$.
2. $\beta = \alpha^{3688}$. La famille $\beta, ..., \theta^7(\beta)$ est linéairement indépendante sur $\mathbb{F}_2$.
3. Le casoratien de ces éléments est $L_f = X^8 + X^6 + X^2 + 1$ qui est central.
4. On prend $\delta = 1$ et on forme le plus petit espace stable par $\sigma(x) = x^4$ contenant β. Le casoratien d'une base de cet espace est : $L_g = X^4 + w^2X^3 + X^2 + X + 1$.
5. On obtient un code sur $\mathbb{F}_4$ qui a pour matrice génératrice :
$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$
6. $[8, 4, 4]$ code, c'est un θ-code. Il descend en un [16,8,4] code sur $\mathbb{F}_2$.

Un exemple détaillé

1. $\mathbb{F}_4$, $\theta(x) = x^2$, $s = 6$ et $\sigma(x) = x^4$.
2. $\beta = \alpha^{3688}$. La famille $\beta, ..., \theta^7(\beta)$ est linéairement indépendante sur $\mathbb{F}_2$.
3. Le casoratien de ces éléments est $L_f = X^8 + X^6 + X^2 + 1$ qui est central.
4. On prend $\delta = 1$ et on forme le plus petit espace stable par $\sigma(x) = x^4$ contenant β. Le casoratien d'une base de cet espace est : $L_g = X^4 + w^2X^3 + X^2 + X + 1$.
5. On obtient un code sur $\mathbb{F}_4$ qui a pour matrice génératrice :
$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$
6. $[8, 4, 4]$ code, c'est un θ-code. Il descend en un [16,8,4] code sur $\mathbb{F}_2$.

Un exemple détaillé

1. $\mathbb{F}_4$, $\theta(x) = x^2$, $s = 6$ et $\sigma(x) = x^4$.
2. $\beta = \alpha^{3688}$. La famille $\beta, ..., \theta^7(\beta)$ est linéairement indépendante sur $\mathbb{F}_2$.
3. Le casoratien de ces éléments est $L_f = X^8 + X^6 + X^2 + 1$ qui est central.
4. On prend $\delta = 1$ et on forme le plus petit espace stable par $\sigma(x) = x^4$ contenant β. Le casoratien d'une base de cet espace est : $L_g = X^4 + w^2X^3 + X^2 + X + 1$.
5. On obtient un code sur $\mathbb{F}_4$ qui a pour matrice génératrice :
$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$
6. $[8, 4, 4]$ code, c'est un θ-code. Il descend en un [16,8,4] code sur $\mathbb{F}_2$.

Un exemple détaillé

1. $\mathbb{F}_4$, $\theta(x) = x^2$, $s = 6$ et $\sigma(x) = x^4$.
2. $\beta = \alpha^{3688}$. La famille $\beta, ..., \theta^7(\beta)$ est linéairement indépendante sur $\mathbb{F}_2$.
3. Le casoratien de ces éléments est $L_f = X^8 + X^6 + X^2 + 1$ qui est central.
4. On prend $\delta = 1$ et on forme le plus petit espace stable par $\sigma(x) = x^4$ contenant β. Le casoratien d'une base de cet espace est : $L_g = X^4 + w^2X^3 + X^2 + X + 1$.
5. On obtient un code sur $\mathbb{F}_4$ qui a pour matrice génératrice :
$$\begin{pmatrix} 1 & 1 & 1 & w^2 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & w & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & w^2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & w & 1 \end{pmatrix}$$
6. $[8, 4, 4]$ code, c'est un θ-code. Il descend en un [16,8,4] code sur $\mathbb{F}_2$.

Résultats 1

Codes définis sur $\mathbb{F}_8$, $\theta(x) = x^2$.

	$\delta = 1$	$\delta = 2$
$\mathbb{F}_8$	$[3,2,2]_g(3)$	$[3,1,3]_g(3)$
$\mathbb{F}_{8^2}$	$[6,4,3]_g(9)$ $[6,4,2]_g(3)$	$[6,2,3]_g(3)$ $[6,2,5]_g(9)$
$\mathbb{F}_{8^3}$	$[9,6,3]_g(54)$ $[9,6,4]_g(9)$ $[6,4,3](21)$	$[9,3,6]_g(54)$ $[6,2,5](21)$
$\mathbb{F}_{8^4}$	$[12,8,2]_g(3)$ $[12,8,3]_g(63)$ $[12,8,4]_g(126)$ $[9,6,2](3)$ $[9,6,3](45)$	$[12,4,3]_g(3)$ $[12,4,5]_g(9)$ $[12,4,6]_g(54)$ $[12,4,7]_g(54)$ $[12,4,8]_g(72)$ $[9,3,3](3)$ $[9,3,5](9)$ $[9,3,6](36)$

Résultats 2

Codes définis sur $\mathbb{F}_{16}$, $\theta(x) = x^4$.

	$\delta = 1$
$\mathbb{F}_{16}$	$[2,1,2]_g(4)$
$\mathbb{F}_{16^2}$	$[4,2,3]_g(16)$
$\mathbb{F}_{16^3}$	$[6,3,2]_g(4)$ $[6,3,4]_g(1)$ $[4,2,2](12)$ $[4,2,3](36)$
$\mathbb{F}_{16^4}$	$[8,4,4]_g(64)$ $[8,4,5]_g(192)$ $[6,3,4]_g(64)$

Exemples de bons codes

1. $[21, 14, 6]$ sur $\mathbb{F}_8$ issu de $\mathbb{F}_{8^8}$ avec :

$$g = X^7 + wX^6 + w^3X^5 + w^5X^4 + w^6X^3 + w^4X^2 + w$$

$$f = X^{21} + X^{18} + X^{15} + X^{12} + X^9 + X^6 + X^3 + 1$$

2. $[21, 14, 6]$ sur $\mathbb{F}_8$ issu de $\mathbb{F}_{8^7}$ avec :

$$g = X^7 + wX^6 + w^3X^5 + w^4X^4 + w^5X^3 + w^3X^2 + wX + w^2$$

$$f = X^{21} + 1$$

Exemples de bons codes

1. $[21, 14, 6]$ sur $\mathbb{F}_8$ issu de $\mathbb{F}_{8^8}$ avec :

$$g = X^7 + wX^6 + w^3X^5 + w^5X^4 + w^6X^3 + w^4X^2 + w$$

$$f = X^{21} + X^{18} + X^{15} + X^{12} + X^9 + X^6 + X^3 + 1$$

2. $[21, 14, 6]$ sur $\mathbb{F}_8$ issu de $\mathbb{F}_{8^7}$ avec :

$$g = X^7 + wX^6 + w^3X^5 + w^4X^4 + w^5X^3 + w^3X^2 + wX + w^2$$

$$f = X^{21} + 1$$

Un très bon code

$[42, 14, 21]$ sur $\mathbb{F}_8$ issu de $\mathbb{F}_{8^{14}}$

Améliore la meilleure distance minimale connue auparavant.

BCH tordus

Analogie avec les BCH classiques en imposant des facteurs à droite de la forme :

$$X - \alpha, ..., \ X - \alpha^{\delta}$$

Résultats sur $\mathbb{F}_8$

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

Un très bon code

$[40, 23, 10]$ sur $\mathbb{F}_4$ issu de $\mathbb{F}_{4^{20}}$
Améliore la meilleure distance minimale connue auparavant.

Skew codes of prescribed distance or rank.
L. Chaussade, P. Loidreau et F.Ulmer.
A paraître dans : Designs, Codes and Cryptography .