Autour de codes définis à l'aide de polynômes tordus.

avec Willi Geiselmann et Felix Ulmer

D. Boucher, IRMAR, Université Rennes 1

JNCF, 4-8 février 2019

Première partie I

Généralités sur les codes modules tordus.

F corps fini

Définition

C, code linéaire de longueur n et de dimension k : sev de F^n de dimension k.

Matrice génératrice $G \in M_{k,n}(F)$, $\mathrm{rang}(G) = k$

$$C = \{m \times G \mid m \in F^k\}$$

Distance minimale de C :

$$d := \min_{x,y \in C, x \neq y} d_H(x,y) = \min_{x \in C, x \neq 0} d_H(x,0)$$

où $d_H(x,y) := \#\{i \mid x_i \neq y_i\}$

notation $[n,k,d]_q$

Théorème de la borne de Singleton : $d \leq n-k+1$

Définition

Soit $C \subset F^n$. Le dual $C^\perp$ de C est :

$$C^\perp := \{x \in F^n \mid \forall c \in C, < x, c >= 0\}$$

où $\forall x, y \in F^n$,

$$< x, y >:= \sum_{i=0}^{n-1} x_i y_i.$$

Matrice de contrôle H de C : matrice génératrice de $C^\perp$

$$C = \{x \in F^n \mid H \times {}^t x = 0\}$$

Exemples de familles de codes :

- Codes MDS : $d = n - k + 1$

  ex : codes de Reed-Solomon, Reed-Solomon généralisés, codes de Gabidulin

- Codes auto-duaux : $C = C^{\perp}$

  ex : codes auto-duaux de Sloane, Thompson ; Gaborit, Otmani ; Harada, etc

But de ce cours : présentation de quelques travaux réalisés avec Willi Geiselmann et Felix Ulmer sur les codes tordus :

codes cycliques tordus autoduaux

codes d'évaluation tordue MDS

Définition (codes θ-cycliques, [BGU 2007]-)

- F, corps fini ; $n \in \mathbb{N}^*$; $\theta \in Aut(F)$
- $C \subset F^n$, code linéaire
- C est un *code θ-cyclique* si $\forall (c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in F^n$,

$$(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \in C \Rightarrow (\theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in C$$

- Si $\theta = Id$, alors C est un code cyclique.
- Si $F = \mathbb{F}_{q^n}$ et $\theta : a \mapsto a^q$, alors C est un code q-cyclique de Gabidulin (1985).

- $R = F[X;\theta]$ anneau des polynômes tordus (Ore, 1933) défini par

$$\forall a \in F, X \cdot a = \theta(a)X.$$

- R est un anneau euclidien à droite et à gauche.
  existence de $\mathrm{lcrm}, \mathrm{lclm}, \mathrm{gcld}, \mathrm{gcrd}$
- Soit $F^\theta = Fix(\theta)$ et soit $m = ord(\theta)$. Les éléments de $F^\theta[X^m]$ sont *centraux* :

$$\forall a \in F, X^m \cdot a = \theta^m(a)X^m = aX^m$$

$R = F[X]$

$$\begin{array}{cccc} R/(X^n - 1) & \text{anneau quotient} & \leftrightarrow & F^n \\ \cup & & & \cup \\ (g)/(X^n - 1) & \text{idéal principal} & \leftrightarrow & C \quad \text{code cyclique} \\ \updownarrow & & & \\ g | X^n - 1 & & & \\ g \text{ unitaire} & & & \end{array}$$

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

$R = F[X;\theta]$, $\theta \in Aut(F)$

$$\begin{array}{cccc}
R/R(X^n-1) & R\text{-module à gauche} & \leftrightarrow & F^n \\
\cup & & & \cup \\
Rg/R(X^n-1) & R\text{-sous-module à gauche} & \leftrightarrow & C = (g)_{n,\theta,c} \quad \text{code } \theta\text{-cyclique} \\
\updownarrow & & & \\
g|_r X^n - 1 & & & \\
g \text{ unitaire} & & &
\end{array}$$

Codes $[2,1]_4$ cycliques et θ-cycliques

$\mathbb{F}_4 = \mathbb{F}_2(a), a^2 + a + 1 = 0, \theta : x \mapsto x^2,\ R = \mathbb{F}_4[X;\theta]$

- Les facteurs de degré 1 de $X^2 - 1$ dans $\mathbb{F}_4[X]$:

$$X^2 - 1 = (X+1)(X+1) \in \mathbb{F}_4[X]$$

- Les facteurs à droite de degré 1 de $X^2 - 1$ dans R :

$$\begin{array}{rcl} X^2 - 1 & = & (X+1)\cdot(X+1) \\ & = & (X+a^2)\cdot(X+a) \\ & = & (X+a)\cdot(X+a^2) \end{array}$$

Codes $[4,2]_4$ cycliques et θ-cycliques.

$\mathbb{F}_4 = \mathbb{F}_2(a), a^2 + a + 1 = 0, \theta : x \mapsto x^2,\ R = \mathbb{F}_4[X;\theta]$

- Les facteurs de degré 2 de $X^4 - 1$ dans $\mathbb{F}_4[X]$:

$$X^4 - 1 = (X^2 + 1)(X^2 + 1) \in \mathbb{F}_4[X]$$

- Les facteurs à droite de degré 2 de $X^4 - 1$ dans R :

$$\begin{array}{rcl} X^4 - 1 & = & (X^2 + 1) \cdot (X^2 + 1) \\ & = & (X^2 + aX + a^2) \cdot (X^2 + aX + a) \\ & = & (X^2 + a^2X + a) \cdot (X^2 + a^2X + a^2) \\ & = & (X^2 + X + a) \cdot (X^2 + X + a^2) \\ & = & (X^2 + X + a^2) \cdot (X^2 + X + a) \\ & = & (X^2 + a^2X + a^2) \cdot (X^2 + a^2X + a) \\ & = & (X^2 + aX + a) \cdot (X^2 + aX + a^2) \end{array}$$

Codes $[10,5]_4$ cycliques et θ-cycliques.

$\mathbb{F}_4 = \mathbb{F}_2(a), a^2 + a + 1 = 0, \theta : x \mapsto x^2,\ R = \mathbb{F}_4[X;\theta]$

- Les facteurs à droite de degré 5 de $X^{10} - 1$ dans $\mathbb{F}_4[X]$:
  $X^{10} - 1$

$$\begin{aligned} &= (X^5 - 1)(X^5 - 1) \\ &= (X^5 + X^4 + a^2X^3 + a^2X^2 + X + 1)(X^5 + X^4 + aX^3 + aX^2 + X + 1) \\ &= (X^5 + X^4 + aX^3 + aX^2 + X + 1)(X^5 + X^4 + a^2X^3 + a^2X^2 + X + 1) \end{aligned}$$

- Les facteurs à droite de degré 5 de $X^{10} - 1$ dans R :

$$\begin{aligned} X^{10} - 1 &= (X^5 - 1) \cdot (X^5 - 1) \\ &= (X^5 + a) \cdot (X^5 + a^2) \\ &= \vdots \end{aligned}$$

51 facteurs à droite

Deux polynômes g_1 et g_2 de R sont dits similaires ($g_1 \sim g_2$) si les modules à gauche (ou à droite) $R/(g_1)$ et $R/(g_2)$ sont isomorphes ([Jacobon 1943]).

Théorème (Ore, Jacobson)

Soient $h = h_1 \cdots h_m = g_1 \cdots g_n$ deux décompositions en produits d'irréductibles de R. Alors $m = n$ et $\exists \sigma \in S_n, g_{\sigma(i)} \sim h_i$.

Factorisation des polynômes sur R :

[Ore, 1933], [Jacobson, 1943], [Giesbrecht, 1998], [Odoni, 1999], [Coulter, Havas, Henderson, 2004],[Caruso, Leborgne, 2012], ...

$R = F[X;\theta]$, $\theta \in Aut(F)$

$$\begin{array}{cccc} R/R(X^n+1) & R\text{-module à gauche} & \leftrightarrow & F^n \\ \cup & & & \cup \\ Rg/R(X^n+1) & R\text{-sous-module à gauche} & \leftrightarrow & C = (g)_{n,\theta,nc} \quad \theta\text{-négacyclique} \\ \updownarrow & & & \\ g|_r X^n+1 & & & \\ g \text{ unitaire} & & & \end{array}$$

$R = F[X;\theta]$, $\theta \in Aut(F)$

$$\begin{array}{ccccc} R/R(X^n - a), a \in F^* & R\text{-module à gauche} & \leftrightarrow & F^n & \\ \cup & & & \cup & \\ Rg/R(X^n - a) & R\text{-sous-module à gauche} & \leftrightarrow & C = (g)^a_{n,\theta} & \theta\text{-constacyc.} \\ \updownarrow & & & & \\ g|_r X^n - a & & & & \\ g \text{ unitaire} & & & & \end{array}$$

$R = F[X;\theta]$, $\theta \in Aut(F)$

$$\begin{array}{cccc} R/Rf, \deg(f) = n & R\text{-module à gauche} & \leftrightarrow & F^n \\ \cup & & & \cup \\ Rg/Rf & R\text{-sous-module à gauche} & \leftrightarrow & C = (g)_{n,\theta} \quad \theta\text{-code module} \\ \updownarrow & & & \\ g|_r f & & & \\ g \text{ unitaire, } g_0 \neq 0 & & & \end{array}$$

Définition (θ-codes modules)

- F, corps fini ; $n \in \mathbb{N}^*$; $\theta \in Aut(F)$ et $C \subset F^n$
- C est un *θ-code module* si $\exists\ g(X) \in R = F[X;\theta]$ tel que

$$\boxed{(c_0, \ldots, c_{n-1}) \in C \Leftrightarrow g(X) \mid_r c_0 + \cdots + c_{n-1}X^{n-1}.}$$

- Une matrice génératrice de C est

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

θ-code module

$$C = (g)_{n,\theta},\ g_0 \neq 0$$

θ-constacyclique

$$\exists a \in F, g|_r X^n - a$$

$$C = (g)^a_{n,\theta}$$

θ-cyclique raccourci

$\exists N \in \mathbb{N}, g|_r X^N - 1$ (notion de borne)

$$C = rac((g)^1_{N,\theta})$$

Définition

Soit $h = \sum_{i=0}^{k} h_i X^i \in R$. Le polynôme réciproque (tordu) de h est

$$h^* = \sum_{i=0}^{k} X^{k-i} \cdot h_i.$$

Le polynôme réciproque (tordu) unitaire de h est

$$h^\natural = \frac{1}{\theta^k(h_0)} \sum_{i=0}^{k} X^{k-i} \cdot h_i.$$

Exemple dans $\mathbb{F}_4[X;\theta]$ avec $\theta : x \mapsto x^2 \in Aut(\mathbb{F}_4)$

$$h = X^2 + aX + a$$

$$h^* = 1 + X \cdot a + X^2 \cdot a = 1 + a^2 X + aX^2$$

$$h^\natural = X^2 + aX + a^2$$

Proposition

Le dual d'un code θ-constacyclique est un code θ-constacyclique.

Démonstration.

Soit $g = \sum_{i=0}^{n-k} g_i X^i \in R$ unitaire et soit $C = (g)^a_{n,\theta}$

$$\exists h \in F[X;\theta], \quad \Theta^n(h) \cdot g = X^n - a \quad \Leftrightarrow \quad \boxed{C = (g)^a_{n,\theta}}$$

$\deg(h) = k$

$$\Updownarrow$$

$$g \cdot h = X^n - \theta^{-k}(a) \quad \overbrace{\Rightarrow}^{(*)} \quad C^\perp = (h^*)_{n,\theta}$$

$$\Updownarrow$$

$$-\frac{1}{a}\Theta^{k-n}(g^*) \cdot h^* = X^n - \frac{1}{a} \quad \Rightarrow \quad (h^*)_{n,\theta} = \boxed{(h^*)^{1/a}_{n,\theta} = C^\perp}$$

$(*) < X^i \cdot g, X^j \cdot h^* >= \theta^i\left((g \cdot h)_\ell\right)$ □

θ-code module

$$C = (g)_{n,\theta},\ g_0 \neq 0$$

θ-constacyclique

$$C = (g)^{a}_{n,\theta}$$

dual

θ-constacyclique

$$C^{\perp} = (h^{*})^{1/a}_{n,\theta}$$

θ-cyclique raccourci

dual

θ-cyclique poinçonné

Proposition

Un θ-code module auto-dual est ou bien θ-cyclique ou bien θ-négacyclique.

Démonstration.

$C = (g)_{n,\theta}$ auto-dual

$$\Rightarrow (g)^a_{n,\theta} = C = C^\perp = (h^*)^{1/a}_{n,\theta}$$

$$\Rightarrow g|_r X^n - a \text{ et } g|_r X^n - \frac{1}{a}$$

$$\Rightarrow a = \frac{1}{a}$$

$$\Rightarrow a = 1 \text{ ou } a = -1$$

□

Deuxième partie II

Codes auto-duaux θ-cycliques.

But de la partie II :

- Donner une intepprétation polynomiale des codes θ-cycliques auto-duaux : équation auto-duale dans R
- Existence de solutions de l'équation auto-duale
- Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension p^s
- Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension quelconque

1. Equation auto-duale.

2. Existence des solutions.
   - Existence solutions binomiales.
   - Existence solutions polynomiales.

3. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension p^s.

4. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension non divisible par p.

5. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension quelconque.

Lemme technique

Soit $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^m})$ et soit $\ell = \mathrm{pgcd}(n, m)$.

$$\left\{ \begin{array}{l} h|_r X^n - 1 \\ h \in \mathbb{F}_{p^m}[X;\theta] \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} h|_r X^n - 1 \\ h \in \mathbb{F}_{p^\ell}[X;\theta] \end{array} \right.$$

Conséquence

Sans perte de généralité, on peut supposer que m divise $n = 2k$. On note

$$2k = m \times p^s \times t, p \not| t$$

Equation auto-duale.

Le code θ-cyclique $(g)^{\theta}_{n=2k}$ est auto-dual si et seulement si $g = h^{\natural}$ où $h = X^k + \cdots + \alpha$ unitaire vérifie :

$$\boxed{h^{\natural} \cdot h = h \cdot h^{\natural} = X^{2k} - 1}$$: équation auto-duale

et $h^{\natural} := \dfrac{1}{\theta^k(\alpha)} h^*$.

Codes $[4,2]_4$ θ-cycliques auto-duaux

$F = \mathbb{F}_4 = \mathbb{F}_2(a), a^2 + a + 1 = 0, \theta : x \mapsto x^2$

Les factorisations de $X^4 - 1$ en produits de deux polynômes tordus de degré 2 :

$$\begin{array}{rcl} X^4 - 1 & = & (X^2+1)\cdot(X^2+1) \\ & = & (X^2+aX+a^2)\cdot(X^2+aX+a) \\ & = & (X^2+a^2X+a)\cdot(X^2+a^2X+a^2) \\ & = & (X^2+X+a)\cdot(X^2+X+a^2) \\ & = & (X^2+X+a^2)\cdot(X^2+X+a) \\ & = & (X^2+a^2X+a^2)\cdot(X^2+a^2X+a) \\ & = & (X^2+aX+a)\cdot(X^2+aX+a^2) \end{array}$$

Codes $[10,5]_4$ θ-cycliques auto-duaux

$F = \mathbb{F}_4 = \mathbb{F}_2(a), a^2 + a + 1 = 0, \theta : x \mapsto x^2$

$$
\begin{aligned}
X^{10} - 1 & \\
&= (X^5 + 1) \cdot (X^5 + 1) \\
&= (X^5 + X^4 + a^2X^3 + a^2X^2 + X + 1) \cdot (X^5 + X^4 + a^2X^3 + aX^2 + X + 1) \\
&= (X^5 + X^4 + aX^3 + aX^2 + X + 1) \cdot (X^5 + X^4 + aX^3 + a^2X^2 + X + 1) \\
&= (X^5 + aX^4 + aX^3 + aX^2 + aX + 1) \cdot (X^5 + a^2X^4 + aX^3 + a^2X^2 + aX + 1) \\
&= (X^5 + a^2X^4 + a^2X^3 + a^2X^2 + a^2X + 1) \cdot (X^5 + aX^4 + a^2X^3 + aX^2 + a^2X + 1) \\
&= (X^5 + a) \cdot (X^5 + a^2) \\
&\vdots
\end{aligned}
$$

$\rightarrow$ 5 codes θ-cycliques auto-duaux $[10,5]_4$.

Codes θ-cycliques auto-duaux de dimension 1 sur $\mathbb{F}_{p^m}$ avec $\theta : x \mapsto x^p$.

$$\underbrace{(X + 1/\theta(\alpha))}_{h^\natural} \cdot \underbrace{(X+\alpha)}_{h} = X^2 - 1 \Leftrightarrow \alpha^2 = -1 \text{ et } \alpha^{p-1} = -1$$

- $p = 2$: 1 solution $X + 1$
- $p \equiv 3 \pmod 4$ et m pair : 2 solutions $X + \alpha, \alpha^2 = -1$
- $p \equiv 3 \pmod 4$ et m impair : 0 solution
- $p \equiv 1 \pmod 4$: 0 solution

Codes θ-cycliques auto-duaux de dimension k fixée.

- $C = (g)_{2k,\theta}$ avec $\deg(g(X)) = k$

- $C = C^{\perp} \Leftrightarrow h^{\natural} \cdot h = X^{2k} - 1,\ h^{\natural} = g$

$\rightarrow \left\lfloor \frac{k}{2} \right\rfloor + 1$ équations polynomiales et inconnues

Codes θ-cycliques auto-duaux sur $\mathbb{F}_4$ de longueur ≤ 50

longueur	nbr cyc.	meilleure dist. cyc.	nbr θ-cyc.	meilleure dist. θ-cyc.	meilleure dist. connue
4	1	2	3	3	3
6	3	3	3	3	3
8	**1**	**2**	**3**	**4**	4
10	1	2	5	4	4
12	5	4	21	6	6
14	3	4	11	6	6
16	**1**	**2**	**3**	**4**	6
18	9	4	27	6	6
20	1	2	63	8	8
22	3	6	33	8	8
24	9	4	93	7	8
26	1	2	65	8	8
28	5	4	279	9	9
30	27	6	285	10	10
32	**1**	**2**	**3**	**4**	10
34	1	2	289	10	10
36	25	6	1 533	11	11
38	3	8	513	11	11
40	1	2	1 023	12	12
42	81	10	2 211	12	12
44	5	6	3 171	14	14
46	3	8	2 051	14	14
48	17	4	1 533	12	14
50	1	2	5 125	14	14

Codes θ-cycliques auto-duaux sur $\mathbb{F}_9$ de longueur ≤ 30

longueur	nbr θ-cyc.	meilleure dist. θ-cyc.	meilleure dist. connue
4	0		3
6	**8**	**4**	4
8	0		5
10	20	5	6
12	0		6
14	56	6	6
16	0		8
18	**242**	**8**	8
20	0		10
22	492	9	9
24	0		10
26	1800	10	10
28	0		12
30	6560	11	12

Codes θ-cycliques auto-duaux sur $\mathbb{F}_{25}$ de longueur ≤ 30

Pas de code !

1. Equation auto-duale.

2. Existence des solutions.
   - Existence solutions binomiales.
   - Existence solutions polynomiales.

3. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension p^s.

4. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension non divisible par p.

5. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension quelconque.

Solutions binomiales : motivation

- Les binômes sont plus simples !
- Si $p = 2$

$$\begin{array}{rcl} (X^k+1)^\natural \cdot (X^k+1) & = & (1+X^k)\cdot(X^k+1) \\ & = & X^{2k}+1 \end{array}$$

$\rightarrow$ il existe un code θ-cyclique auto-dual de dimension k sur $\mathbb{F}_{2^m}$ (pour tout θ).

- Si p est impair et $\theta = id$

$$\begin{array}{rcl} (X^k+\alpha)^\natural \cdot (X^k+\alpha) & = & (X^k+\frac{1}{\alpha})\cdot(X^k+\alpha) \\ & \neq & X^{2k}-1 \end{array}$$

$\rightarrow$ il n'existe pas de code cyclique "binomial" auto-dual de dimension k sur $\mathbb{F}_{p^m}$ avec p impair.

Que dire si p est impair et $\theta : x \mapsto x^p$?

On suppose que p est impair.
Soit $k \in \mathbb{N}^*$.
Soit $h = X^k + \alpha \in R$ tel que $\alpha \neq 0$ et $h^\natural \cdot h = X^{2k} - 1$.

$$h^* = X^{k-k} \cdot 1 + X^{k-0} \cdot \alpha = 1 + \theta^k(\alpha) X^k$$

$$h^\natural = X^k + \frac{1}{\theta^k(\alpha)}$$

$$\begin{aligned} h^\natural \cdot h &= \left(X^k + \frac{1}{\theta^k(\alpha)}\right) \cdot (X^k + \alpha) \\ &= X^{2k} + X^k \cdot \alpha + \frac{1}{\theta^k(\alpha)} X^k + \frac{\alpha}{\theta^k(\alpha)} \\ &= X^{2k} + \left(\theta^k(\alpha) + \frac{1}{\theta^k(\alpha)}\right) X^k + \frac{\alpha}{\theta^k(\alpha)} \end{aligned}$$

On suppose que p est impair.
Soit $k \in \mathbb{N}^*$.
Soit $h = X^k + \alpha \in R$ tel que $\alpha \neq 0$ et $h^\natural \cdot h = X^{2k} - 1$.

$$h^* = X^{k-k} \cdot 1 + X^{k-0} \cdot \alpha = 1 + \theta^k(\alpha) X^k$$

$$h^\natural = X^k + \frac{1}{\theta^k(\alpha)}$$

$$\begin{aligned} h^\natural \cdot h &= \left(X^k + \frac{1}{\theta^k(\alpha)} \right) \cdot (X^k + \alpha) \\ &= X^{2k} + X^k \cdot \alpha + \frac{1}{\theta^k(\alpha)} X^k + \frac{\alpha}{\theta^k(\alpha)} \\ &= X^{2k} + \left(\theta^k(\alpha) + \frac{1}{\theta^k(\alpha)} \right) X^k + \frac{\alpha}{\theta^k(\alpha)} \end{aligned}$$

On suppose que p est impair.
Soit $k \in \mathbb{N}^*$, $\alpha \in \mathbb{F}_q \setminus \{0\}$ et $h = X^k + \alpha \in R$.

$$
\begin{aligned}
h^\natural \cdot h = X^{2k} - 1 \quad & \Leftrightarrow \quad \theta^k(\alpha) + \frac{1}{\theta^k(\alpha)} = 0 \text{ et } \frac{\alpha}{\theta^k(\alpha)} = -1 \\
& \Leftrightarrow \quad \alpha + \frac{1}{\alpha} = 0 \text{ et } 1 = -\theta^k(\alpha)/\alpha \\
& \Leftrightarrow \quad \alpha^2 = -1 \text{ et } 1 = -\alpha^{p^k - 1} \\
& \Leftrightarrow \quad \alpha^2 = -1 \text{ et } 1 = (-1)^{\frac{p^k+1}{2}} \\
& \Leftrightarrow \quad \alpha^2 = -1, p^k \equiv 3 \pmod 4
\end{aligned}
$$

Conditions d'existence de codes auto-duaux "binomiaux" θ-cycliques de dimension $k \in \mathbb{N}^*$ sur $\mathbb{F}_{q=p^m}$ avec p nombre premier impair et $\theta : x \mapsto x^p$.

$$p \equiv 3 \pmod 4, m \equiv 0 \pmod 2, k \equiv 1 \pmod 2$$

1. Equation auto-duale.

2. Existence des solutions.
   - Existence solutions binomiales.
   - Existence solutions polynomiales.

3. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension p^s.

4. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension non divisible par p.

5. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension quelconque.

$\boxed{h^{\natural} \cdot h = X^{2k} - 1}$: équation auto-duale

Point de vue insipiré de

- Sloane et Thompson (codes cycliques auto-duaux)
- et de Giesbrecht (factorisation des polynômes tordus)

$\rightarrow$ écriture des solutions sous forme de ppcm à droite (lcrm)
$\rightarrow$ conditions nécessaires et suffisantes d'existence

Théorème [Sloane, Thompson, 1983], [Jia, Ling, Xing, 2011]

Soit s tel que $p^{s+1}||n=2k$ et soit $T(n)$ le nombre de polynômes $f=g\times g^\natural$ tels que $g^\natural\neq g$ soit irréductible et divise X^n-1 dans $\mathbb{F}_{p^m}[X]$. Le nombre de codes cycliques auto-duaux de longueur $n=2k$ sur $\mathbb{F}_{p^m}$ est

$$\left\{\begin{array}{ccc} (2^{s+1}+1)^{T(n)} & \text{si} & p=2 \\ 0 & \text{si} & p \text{ impair.} \end{array}\right.$$

Preuve

Soit s tel que $p^{s+1}||2k$.

$$X^{2k}-1=\prod_{f_i=f_i^\natural,\ f_i\ irr} f_i(X)^{p^{s+1}} \prod_{f_i=g_ig_i^\natural, g_i\neq g_i^\natural\ irr} f_i(X)^{p^{s+1}} \in \mathbb{F}_q[X]$$

$$h^\natural\cdot h=X^{2k}-1 \quad\Leftrightarrow\quad \begin{array}{l} h=\prod h_i \\ h_i^\natural\cdot h_i=f_i(X)^{p^{s+1}} \end{array}$$

$$h_i^\natural\cdot h_i=f_i(X)^{p^{s+1}} \quad\Leftrightarrow\quad \begin{array}{lll} h_i=f_i(X)^{2^s} & \text{si} & f_i \quad \text{irréductible} \\ h_i=g_i(X)^{\beta_i}(g_i^\natural(X))^{2^{s+1}-\beta_i} & \textit{sinon} & \end{array}$$

Théorème [Sloane, Thompson, 1983], [Jia, Ling, Xing, 2011]

Soit s tel que $p^{s+1}||n = 2k$ et soit $T(n)$ le nombre de polynômes $f = g \times g^\natural$ tels que $g^\natural \neq g$ soit irréductible et divise $X^n - 1$ dans $\mathbb{F}_{p^m}[X]$. Le nombre de codes cycliques auto-duaux de longueur $n = 2k$ sur $\mathbb{F}_{p^m}$ est

$$\begin{cases} (2^{s+1}+1)^{T(n)} & \text{si} \quad p = 2 \\ 0 & \text{si} \quad p \text{ impair.} \end{cases}$$

Preuve

Soit s tel que $p^{s+1}||2k$.

$$X^{2k} - 1 = \prod_{f_i = f_i^\natural,\ f_i\ irr} f_i(X)^{p^{s+1}} \prod_{f_i = g_i g_i^\natural, g_i \neq g_i^\natural\ irr} f_i(X)^{p^{s+1}} \in \mathbb{F}_q[X]$$

$$h^\natural \cdot h = X^{2k} - 1 \quad \Leftrightarrow \quad \begin{array}{l} h = \prod h_i = \mathrm{ppcm}(h_i) \\ h_i^\natural \cdot h_i = f_i(X)^{p^{s+1}} \end{array}$$

$$h_i^\natural \cdot h_i = f_i(X)^{p^{s+1}} \quad \Leftrightarrow \quad \begin{array}{ll} h_i = f_i(X)^{2^s} & \text{si} \quad f_i \quad \text{irréductible} \\ h_i = g_i(X)^{\beta_i}(g_i^\natural(X))^{2^{s+1}-\beta_i} & \textit{sinon} \end{array}$$

Nombres de codes cycliques auto-duaux sur $\mathbb{F}_2$, $\mathbb{F}_4$, $\mathbb{F}_8$ et $\mathbb{F}_{16}$.

Dimension	$\mathbb{F}_2$	$\mathbb{F}_4$	$\mathbb{F}_8$	$\mathbb{F}_{16}$
2^s	1	1	1	1
$2^s \times 3$	1	$1 + 2^{s+1}$	1	$1 + 2^{s+1}$
$2^s \times 5$	1	1	1	$(1 + 2^{s+1})^2$
$2^s \times 7$	$1 + 2^{s+1}$	$1 + 2^{s+1}$	$(1 + 2^{s+1})^3$	$1 + 2^{s+1}$
$2^s \times 9$	1	$(1 + 2^{s+1})^2$	1	$(1 + 2^{s+1})^2$
$\dots$				

Codes cycliques autoduaux $[10, 5]$ sur $\mathbb{F}_4$.

$$X^{10} - 1 = (\underbrace{X - 1}_{irr})^2 \, (\underbrace{X^2 + aX + 1}_{f = f^\natural, irr})^2 \, (\underbrace{X^2 + a^2 X + 1}_{f = f^\natural, irr})^2 \in \mathbb{F}_4[X]$$

$(1+2)^0 = 1$ code autodual cyclique engendré par $h^\natural$ où

$$h = (X+1)(X^2 + aX + 1)(X^2 + a^2 X + 1) = X^5 + 1.$$

Proposition

Soit $R = \mathbb{F}_{p^m}[X;\theta]$ avec $\theta : x \mapsto x^p$.
On suppose $n = 2k = m \times p^s \times t$, $p \not| t$ et on considère

$$X^{2k} - 1 = ((X^m)^t - 1)^{p^s} = \prod_{f_i = f_i^\natural,\ f_i\ irr} f_i(X^m)^{p^s} \prod_{f_i = g_i g_i^\natural, g_i \neq g_i^\natural\ irr} f_i(X^m)^{p^s} \in \mathbb{F}_p[X^m]$$

$$h^\natural \cdot h = X^{2k} - 1 \in R \quad \Leftrightarrow \quad \begin{array}{l} h = \mathrm{lcrm}(h_i) \\ h_i^\natural \cdot h_i = f_i(X^m)^{p^s} \in R \end{array}$$

Preuve

$h = \mathrm{lcrm}(h_i)$ avec $h_i = \mathrm{gcld}(h, f_i(X^m)^{p^s})$ (d'après [Giesbrecht, 1998])

Conséquence

S'il existe un code θ-cyclique auto-dual alors $\exists H \in R, H^\natural \cdot H = (X^m - 1)^{p^s}$.

Supposons que $H = X^K + \cdots + \alpha$ est solution de

$$H^\natural \cdot H = X^{2K} - 1 = (X^m - 1)^{p^s}.$$

alors $m \equiv 0 \pmod 2$.

- $\alpha/\theta^K(\alpha) = -1$
- $H = (X + \alpha_1) \cdots (X + \alpha_K), \alpha_i \in \mathbb{F}_q$
- $N_{2K}(\alpha_i) = 1$ ([Lam 86]) avec $N_{2K}(x) := \theta^{2K-1}(x) \cdots \theta^2(x)\theta(x)x$
- $N_{2K}(\alpha) = 1$

Supposons que $H = X^K + \cdots + \alpha$ est solution de

$$H^{\natural} \cdot H = X^{2K} - 1 = \underbrace{(X^m - 1)}_{deg\ 1\ \in \mathbb{F}_p[X^m]}{}^{p^s}$$

alors $m \equiv 0 \pmod 2$.

- $\alpha / \theta^K(\alpha) = -1$
- $H = (X + \alpha_1) \cdots (X + \alpha_K), \alpha_i \in \mathbb{F}_q$
- $N_{2K}(\alpha_i) = 1$ ([Lam 86]) avec $N_{2K}(x) := \theta^{2K-1}(x) \cdots \theta^2(x)\theta(x)x$
- $N_{2K}(\alpha) = 1$

Supposons que $H = X^K + \cdots + \alpha$ est solution de

$$H^\natural \cdot H = X^{2K} - 1 = (X^m - 1)^{p^s}.$$

alors $m \equiv 0 \pmod 2$.

- $\alpha/\theta^K(\alpha) = -1$
- $H = (X + \alpha_1) \cdots (X + \alpha_K), \alpha_i \in \mathbb{F}_q$
- $N_{2K}(\alpha_i) = 1$ ([Lam 86]) avec $N_{2K}(x) := \theta^{2K-1}(x) \cdots \theta^2(x)\theta(x)x$
- $N_{2K}(\alpha) = 1$

Supposons que $H = X^K + \cdots + \alpha$ est solution de

$$H^\natural \cdot H = X^{2K} - 1 = (X^m - 1)^{p^s}.$$

alors $m \equiv 0 \pmod 2$.

- $\alpha/\theta^K(\alpha) = -1$
- $H = (X + \alpha_1)\cdots(X + \alpha_K), \alpha_i \in \mathbb{F}_q$
- $N_{2K}(\alpha_i) = 1$ ([Lam 86]) avec $N_{2K}(x) := \theta^{2K-1}(x)\cdots\theta^2(x)\theta(x)x$
- $N_{2K}(\alpha) = 1$

On a donc $N_K(\alpha)^{p-1} = -1$ et $N_K(\alpha)^2 = (-1)^K$ d'où $-1 = (-1)^{\frac{p-1}{2}\times K}$ donc

$$p \equiv 3 \pmod 4 \text{ et } m/2 \equiv 1 \pmod 2.$$

Proposition

Il existe un code θ-cyclique auto-dual de dimension k sur $\mathbb{F}_{p^m}$ si et seulement si $p = 2$ ou ($m \equiv 0 \pmod 2$, $k \equiv 1 \pmod 2$ et $p \equiv 3 \pmod 4$).

Preuve (p impair)

On a $n = 2k = m \times p^s \times t$ avec $p \nmid t$.

- S'il y a un code θ-cyclique auto-dual alors
$$\exists H \in R, H^\natural \cdot H = (X^m - 1)^{p^s}$$
donc $m \equiv 0 \pmod 2$, $m/2 \equiv 1 \pmod 2$, $p \equiv 3 \pmod 4$.
De plus
$$\forall H \in R, H^\natural \cdot H \neq (X^m + 1)^{p^s}$$
donc $t \equiv 1 \pmod 2$ donc $k \equiv 1 \pmod 2$.
- Réciproquement, soit $\alpha \in \mathbb{F}_q$ tel que $\alpha^2 = -1$. On a
$$(X^k + \alpha)^\natural \cdot (X^k + \alpha) = X^{2k} + \left(\theta^k(\alpha) + \frac{1}{\theta^k(\alpha)}\right) X^k + \frac{\alpha}{\theta^k(\alpha)} = X^{2k} - 1.$$

Dimension $k = p^s$:

Motivation

- Conjectures sur $\mathbb{F}_4$ et $\mathbb{F}_9$

  3 codes θ-cycliques auto-duaux sur $\mathbb{F}_4$ de dimension 2^s
  $3^* - 1$ codes θ-cycliques auto-duaux sur $\mathbb{F}_9$ de dimension 3^s

- $X^n - 1 = \underbrace{(X^2 - 1)}_{deg\ 1\ \in \mathbb{F}_p[X^2]}{}^{p^s}$

  donc h est un produit de facteurs unitaires linéaires
  $\rightarrow$ degré 1 plus facile que degré quelconque

Principaux outils

- un lemme d'unicité de factorisation ;
- un partitionnement

On suppose que $R = \mathbb{F}_{p^2}[X;\theta]$ avec $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^2})$.
On veut résoudre sur R

$$h^\natural \cdot h = X^{2p^s} - 1 = (X^2 - 1)^{p^s}$$

Rappel $(s = 0)$:

$$h^\natural \cdot h = X^2 - 1 \Leftrightarrow h = X + \alpha \text{ avec } \alpha^2 = -1 \text{ et } \alpha^{p-1} = -1$$

- $p = 2$: 1 solution $X + 1$
- $p \equiv 3 \pmod 4$: 2 solutions $X + \alpha, \alpha^2 = -1$
- $p \equiv 1 \pmod 4$: 0 solution

Code θ-cyclique $[4,2]_4$ auto-dual

$$X^4 - 1 = \underbrace{(X^2 + aX + a^2)}_{h^\natural} \cdot \underbrace{(X^2 + aX + a)}_{h}$$

$$X^4 - 1 = \underbrace{(X + a^2) \cdot (X + 1)}_{\text{unique fact. de } h^\natural} \cdot \underbrace{(X + 1) \cdot (X + a)}_{\text{unique fact. de } h}$$

$$\underbrace{X^4 - 1}_{(X^2-1)^2} = (X + a^2) \cdot \underbrace{(X + 1) \cdot (X + 1)}_{X^2-1} \cdot (X + a)$$

$$X^2 - 1 = \underbrace{(X + a^2) \cdot (X + a)}_{X^2-1}$$

Lemme

Soit $\theta : x \mapsto x^p \in Aut(\mathbb{F}_{p^2})$ et soit $R = \mathbb{F}_{p^2}[X;\theta]$.
Soit $h = (X+\alpha_1)\cdots(X+\alpha_k) \in R$ avec $\alpha_i^{p+1} = 1$ $(X+\alpha_i | X^2-1)$.
Les assertions suivantes sont équivalentes :

(i) La factorisation de h en produit de facteurs linéaires unitaires est unique.

(ii) $X^2 - 1 \not| h$.

(iii) $\forall i \in \{1,\ldots,k-1\}, (X+\alpha_i)\cdot(X+\alpha_{i+1}) \neq X^2-1$ i.e. $\alpha_i\alpha_{i+1} \neq -1$.

Preuve ($k=2$)

Soit $h = (X+\alpha_1)\cdot(X+\alpha_2) \in R$ avec $X+\alpha_i | X^2-1$.
Supposons $\exists \beta_2 \neq \alpha_2, X+\beta_2 |_r h$.
Soit $H = \mathrm{lclm}(X+\alpha_2, X+\beta_2)$.

$$\begin{array}{l} \deg(H) = 2 \\ H |_r h \\ H |_r X^2 - 1 \end{array}$$

donc $H = h = X^2 - 1$.

$$h^\natural \cdot h = (X^2-1)^k, X^2-1 \nmid h$$

$$\Updownarrow$$

$$\underbrace{(X+\tilde{\alpha}_k)\cdots(X+\tilde{\alpha}_1)}_{h^\natural}\cdot\underbrace{(X+\alpha_1)\cdots(X+\alpha_k)}_{h} = (X^2-1)^k$$

avec

$$\begin{cases} \alpha_i^{p+1} = 1 \\ \alpha_i\alpha_{i+1} \neq -1 \\ \\ \tilde{\alpha}_i = \begin{cases} \alpha_i(\alpha_1\cdots\alpha_{i-1})^2 \text{ si } i \text{ impair;} \\ \frac{1}{\alpha_i(\alpha_1\cdots\alpha_{i-1})^2} \text{ si } i \text{ pair.} \end{cases} \end{cases}$$

$$h^{\natural} \cdot h = (X^2 - 1)^k, X^2 - 1 \not| h$$
$$\Downarrow$$
$$(X + \tilde{\alpha}_k) \cdots \underbrace{(X + \tilde{\alpha}_1) \cdot (X + \alpha_1)}_{= X^2 - 1} \cdots (X + \alpha_k) = (X^2 - 1)^k$$

avec

$$\begin{cases} \alpha_i^{p+1} = 1 \\ \alpha_i \alpha_{i+1} \neq -1 \\ \\ \tilde{\alpha}_i = \begin{cases} \alpha_i(\alpha_1 \cdots \alpha_{i-1})^2 \text{ si } i \text{ impair;} \\ \frac{1}{\alpha_i(\alpha_1 \cdots \alpha_{i-1})^2} \text{ si } i \text{ pair.} \end{cases} \\ \\ \alpha_1 \tilde{\alpha}_1 = -1 \text{ donc } \alpha_1^2 = -1 \end{cases}$$

$$h^\natural \cdot h = (X^2-1)^k, X^2-1 \not| h$$
$$\Downarrow$$
$$(X+\tilde{\alpha}_k)\cdots\underbrace{(X+\tilde{\alpha}_2)\cdot(X+\alpha_2)}_{=X^2-1}\cdots(X+\alpha_k) = (X^2-1)^{k-1}$$

avec

$$\begin{cases} \alpha_i^{p+1} = 1 \\ \alpha_i\alpha_{i+1} \neq -1 \\ \\ \tilde{\alpha}_i = \begin{cases} \alpha_i(\alpha_1\cdots\alpha_{i-1})^2 \text{ si } i \text{ impair;} \\ \frac{1}{\alpha_i(\alpha_1\cdots\alpha_{i-1})^2} \text{ si } i \text{ pair.} \end{cases} \\ \\ \alpha_1\tilde{\alpha}_1 = -1 \text{ donc } \alpha_1^2 = -1 \\ \alpha_2\tilde{\alpha}_2 = -1 \end{cases}$$

$$h^\natural \cdot h = (X^2-1)^k,\ X^2-1 \not| h$$

$$\Downarrow$$

$$(X+\tilde{\alpha}_k)\cdots\underbrace{(X+\tilde{\alpha}_3)\cdot(X+\alpha_3)}_{=X^2-1}\cdots(X+\alpha_k) = (X^2-1)^{k-2}$$

avec

$$\left\{\begin{array}{l} \alpha_i^{p+1} = 1 \\ \alpha_i\alpha_{i+1} \neq -1 \\ \\ \tilde{\alpha}_i = \left\{\begin{array}{l} \alpha_i(\alpha_1\cdots\alpha_{i-1})^2 \text{ si } i \text{ impair;} \\ \frac{1}{\alpha_i(\alpha_1\cdots\alpha_{i-1})^2} \text{ si } i \text{ pair.} \end{array}\right. \\ \\ \alpha_1\tilde{\alpha}_1 = -1 \text{ donc } \alpha_1^2 = -1 \\ \alpha_2\tilde{\alpha}_2 = -1 \\ \alpha_3\tilde{\alpha}_3 = -1 \text{ donc } (\alpha_2\alpha_3)^2 = 1 \end{array}\right.$$

$$h^\natural \cdot h = (X^2-1)^k,\ X^2-1 \nmid h$$
$$\Updownarrow$$
$$h = (X+\alpha_1)\cdot(X+\alpha_2)\cdots(X+\alpha_k)$$

avec

$$\begin{cases} \alpha_i^{p+1} = 1 \\ \alpha_i\alpha_{i+1} \neq -1 \\ \alpha_1^2 = -1 \\ \alpha_i\alpha_{i+1} = 1 \text{ si } i \text{ pair.} \end{cases}$$

Nombre de solutions.

$\boxed{p = 2}$

$k > 2$: 0 solution
$k = 2$: 2 solutions
$k = 1$: 1 solution

$\boxed{p \equiv 3 \pmod 4}$

$2p^{\lfloor (k-1)/2 \rfloor}$ solutions

$\boxed{p \equiv 1 \pmod 4}$

0 solution

Lemme

Le nombre de codes θ-cycliques auto-duaux de dimension p^s sur $\mathbb{F}_{p^2}$ avec $s > 0$ est :

$$\begin{cases} 3 & \text{si} \quad p = 2 \\ 2\dfrac{p^{(p^s+1)/2} - 1}{p-1} & \text{si} \quad p \equiv 3 \pmod 4 \\ 0 & \text{si} \quad p \equiv 1 \pmod 4 \end{cases}$$

Preuve

$$h^\natural \cdot h = (X^2-1)^{p^s} \quad \Leftrightarrow \quad \begin{array}{l} \exists i \in \{0, \dots, \lfloor p^s/2 \rfloor\}, \\ h = (X^2-1)^i \cdot H \\ H^\natural \cdot H = (X^2-1)^{p^s-2i}, X^2 - 1 \nmid H \end{array}$$

$$\sum_{i=0}^{(p^s-1)/2} 2p^{(p^s-1-2i)/2} = 2\frac{p^{(p^s+1)/2} - 1}{p-1}$$

Dimension k non divisible par p

Rappel :

Soit $R = \mathbb{F}_{p^2}[X;\theta]$ avec $\theta : x \mapsto x^p$.

$$X^{2k} - 1 = \prod_{f_i = f_i^\natural,\ f_i\ irr} f_i(X^2) \prod_{f_i = g_i g_i^\natural, g_i \neq g_i^\natural\ irr} f_i(X^2) \in \mathbb{F}_p[X^2]$$

$$h^\natural \cdot h = X^{2k} - 1 \in R \quad \Leftrightarrow \quad \begin{array}{l} h = \mathrm{lcrm}(h_i) \\ h_i^\natural \cdot h_i = f_i(X^2) \in R \end{array}$$

Outils : une paramétrisation des irréductibles de R.

$h^\natural \cdot h = f(X^2), f = f^\natural \in \mathbb{F}_p[X^2],\ d = \deg_{X^2}(f)$

- $f(X^2) = X^2 - \epsilon, \epsilon^2 = 1$
  - Pour $\epsilon = 1$, nbe sol :
    2 si $p \equiv 3 \pmod 4$
    0 si $p \equiv 1 \pmod 4$
    1 si $p = 2$
- $f(X^2)$ irr, $d > 1$
  - ?
- $f = g \times g^\natural, g(X^2)$ irr
  - ?

$h^\natural \cdot h = f(X^2), f = f^\natural \in \mathbb{F}_p[X^2],\ d = \deg_{X^2}(f)$

$f(X^2) = X^2 - \epsilon, \epsilon^2 = 1$

2 si $p \equiv -\epsilon \pmod 4$
0 si $p \equiv \epsilon \pmod 4$
1 si $p = 2$

$f(X^2)$ irr, $d > 1$

?

$f = g \times g^\natural, g(X^2)$ irr

?

[Odoni, 1999]

Irreductibles de $\mathbb{F}_p[X^2]$ de degré d en X^2

$f(X^2)$ $\cdots$ $\cdots$

$h(X)$

$1 + p^d$ $1 + p^d$ $1 + p^d$

Irréductibles de $\mathbb{F}_{p^2}[X;\theta]$ de degré d

$$\begin{array}{ccc} \mathbb{F}_{p^2}[X;\theta]/(f(X^2)) & \sim & M_2(\mathbb{F}_{p^d}) \\ h(X) \text{ diviseur de zéro à gauche} & \leftrightarrow & \text{idéal à gauche maximal} \end{array}$$

Soit $f(X^2) \in \mathbb{F}_p[X^2]$, irréductible, $\deg_{X^2} f(X^2) = d$.
Soit $h = A(X^2) + X \cdot B(X^2) \in R$.

$$\underbrace{h}_{\substack{\text{irréd} \\ \text{degré } d}} \quad |_r \quad \underbrace{f(X^2)}_{\substack{\text{produit de 2 irréductibles} \\ 1+p^d \text{ facteurs à droite} \\ \text{(Odoni, 1999)}}}$$

$$\Updownarrow$$

$$B = 0 \text{ et } A(X^2) | f(X^2) \in \mathbb{F}_{p^2}[X^2]$$

ou

$$\frac{A}{B} \equiv P \pmod{f} \in \mathbb{F}_{p^2}(X) \;(\leftarrow \text{interpolation de Cauchy})$$

avec

$$P\Theta(P) \equiv X \pmod{f} \in \mathbb{F}_{p^2}[X]$$

Paramétrisation des $h(X) \in R$ tels que $h^\natural(X) \cdot h(X) = f(X^2)$ avec $f = f^\natural$, $\deg_{X^2} f(X^2) = d = 2\delta$.

Soit $\alpha \in \mathbb{F}_{p^d}$ tel que $f(\alpha) = 0$.

$$h(X) = A(X^2) + X \cdot B(X^2) \mid_r f(X^2)$$

$$\Updownarrow$$

$$\left\{ \begin{array}{l} B = 0 \\ A(X^2) | f(X^2) \end{array} \right. \quad ou \quad \left\{ \begin{array}{l} B \neq 0 \\ \dfrac{A}{B} \equiv P \pmod{f} \end{array} \right.$$

où $P \in \mathbb{F}_{p^2}[X]_{<d}$ est défini par $\left\{ \begin{array}{l} P(\alpha) = u \\ P(\alpha^p) = \alpha^p / u^p \end{array} \right.$ avec $u \in \mathbb{F}_{p^d} \setminus \{0\}$.

Soit $f(X^2) \in \mathbb{F}_p[X^2]$, irréductible, $\deg_{X^2} f(X^2) = d = 2\delta, f = f^\natural$.
Soit $h = A(X^2) + X \cdot B(X^2) \in R$.

$$h^\natural \cdot h = f(X^2)$$

$$\Updownarrow$$

$$B = 0 \text{ et } A(X^2)A^\natural(X^2) = f(X^2)$$

ou

$$\frac{A}{B} \equiv P \pmod{f}$$

avec

$$P\Theta(P) \equiv X \pmod{f} \in \mathbb{F}_{p^2}[X]$$

et

$$X^{2\delta-1}P(1/X) + X^{2\delta-2}\Theta(P)(X) \equiv 0 \pmod{f}$$

Paramétrisation des $h(X) \in R$ tels que $h^\natural(X) \cdot h(X) = f(X^2)$ avec $f = f^\natural$, $\deg_{X^2} f(X^2) = d = 2\delta$ avec δ impair.

Soit $\alpha \in \mathbb{F}_{p^d}$ tel que $f(\alpha) = 0$.

$$h(X) = A(X^2) + X \cdot B(X^2) \text{ solution de } h^\natural(X) \cdot h(X) = f(X^2)$$

$$\Updownarrow$$

$$\left\{ \begin{array}{l} B = 0 \\ A(X^2) | f(X^2) \end{array} \right. \quad ou \quad \left\{ \begin{array}{l} B \neq 0 \\ \dfrac{A}{B} \equiv P \pmod{f} \end{array} \right.$$

où $P \in \mathbb{F}_{p^2}[X]_{<d}$ est défini par $\left\{ \begin{array}{l} P(\alpha) = u \\ P(\alpha^p) = \alpha^p / u^p \end{array} \right.$ avec $u \in \mathbb{F}_{p^d}^*$, $u^{p^\delta - 1} = -\frac{1}{\alpha}$.

Paramétrisation des $h(X) \in R$ tels que $h^\natural(X) \cdot h(X) = f(X^2)$ avec $f = f^\natural$, $\deg_{X^2} f(X^2) = d = 2\delta$ avec δ pair.

Soit $\alpha \in \mathbb{F}_{p^d}$ tel que $f(\alpha) = 0$.

$h(X) = A(X^2) + X \cdot B(X^2)$ solution de $h^\natural(X) \cdot h(X) = f(X^2)$

$$\Updownarrow$$

$$\begin{cases} B \neq 0 \\ \dfrac{A}{B} \equiv P \pmod{f} \end{cases}$$

où P est défini par $\begin{cases} P(\alpha) = u \\ P(\alpha^p) = \alpha^p / u^p \end{cases}$ avec $u \in \mathbb{F}_{p^d}^*$, $u^{p^\delta+1} = -1$.

Résolution de $h^\natural \cdot h = X^8 + X^6 + X^4 + X^2 + 1$ dans $R = \mathbb{F}_4[X;\theta]$.

$h = A(X^2) + X \cdot B(X^2) \in R$ avec

$$\frac{A}{B} \equiv P_u \pmod{f} \in \mathbb{F}_4(X) \text{ et } u \in \mathbb{F}_{16} = \mathbb{F}_2(b), u^5 = 1.$$

u	$P_u(X)$	$A(X)$	$B(X)$	$h = A(X^2) + X \cdot B(X^2)$
1	$X^3 + a^2X + a$	$X^2 + a$	$a^2X + a^2$	$X^4 + aX^3 + aX + a$
b^3	$X^3 + aX + a^2$	$X^2 + a^2$	$aX + a$	$X^4 + a^2X^3 + a^2X + a^2$
b^6	$a^2X^3 + X^2 + aX + a$	$X^2 + 1$	$a^2X + a$	$X^4 + aX^3 + a^2X + 1$
b^{12}	$aX^3 + X^2 + a^2X + a^2$	$X^2 + 1$	$aX + a^2$	$X^4 + a^2X^3 + aX + 1$
b^9	X^3	$X^2 + X + 1$	$X + 1$	$X^4 + X^3 + X^2 + X + 1$

$a^2 + a + 1 = 0$ et $b^4 + b + 1 = 0$

$$h^\natural \cdot h = f(X^2), f = f^\natural \in \mathbb{F}_p[X^2],\ d = \deg_{X^2}(f)$$

- $f(X^2) = X^2 - \epsilon, \epsilon^2 = 1$
  - 2 si $p \equiv -\epsilon \pmod 4$
    0 si $p \equiv \epsilon \pmod 4$
    1 si $p = 2$
- $f(X^2)$ irr, $d > 1$
  - $1 + p^{d/2}$
- $f = g \times g^\natural, g(X^2)$ irr
  - ?

$$h^\natural \cdot h = f(X^2), f = f^\natural \in \mathbb{F}_p[X^2],\ d = \deg_{X^2}(f)$$

$f(X^2) = X^2 - \epsilon, \epsilon^2 = 1$

2 si $p \equiv -\epsilon \pmod 4$
0 si $p \equiv \epsilon \pmod 4$
1 si $p = 2$

$f(X^2)$ irr, $d > 1$

$1 + p^{d/2}$

$f = g \times g^\natural, g(X^2)$ irr

$3 + p^{d/2}$

Proposition

On suppose $p \nmid k$.

$$X^{2k} - 1 = \prod_{f_i = f_i^\natural,\ f_i\ irr} f_i(X^2) \prod_{f_i = g_i g_i^\natural, g_i \neq g_i^\natural\ irr} f_i(X^2) \in \mathbb{F}_p[X^2]$$

Le nombre de codes θ-cycliques auto-duaux sur $\mathbb{F}_{p^2}$ de dimension k est

$$N \times \prod_{f = f^\natural,\ irr, deg > 1} (p^{d/2} + 1) \times \prod_{f = gg^\natural} (p^{d/2} + 3)$$

avec $d := \deg_{X^2}(f(X^2))$ et

$$N = \begin{cases} 1 & \text{si} \quad p = 2 \\ 2 & \text{si} \quad p \equiv 3 \pmod 4 \text{ et } k \equiv 1 \pmod 2 \\ 0 & \text{sinon.} \end{cases}$$

Codes θ-cycliques autoduaux de longueur 10 sur $\mathbb{F}_4$.

$$X^{10} - 1 = (X^2 + 1)(X^8 + X^6 + X^4 + X^2 + 1) \in \mathbb{F}_2[X^2]$$

$$h^\natural \cdot h = X^{10} - 1 \Leftrightarrow h = \mathrm{lcrm}(h_1, h_2)$$

avec

$$\begin{cases} h_1^\natural \cdot h_1 = X^2 - 1 & : 1 \text{ solution} \\ h_2^\natural \cdot h_2 = X^8 + X^6 + X^4 + X^2 + 1 & : 1 + 2^2 \text{ solutions} \end{cases}$$

$\rightarrow$ 5 codes θ-cycliques de longueur 10 autoduaux sur $\mathbb{F}_4$.

1. Equation auto-duale.
2. Existence des solutions.
   - Existence solutions binomiales.
   - Existence solutions polynomiales.
3. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension p^s.
4. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension non divisible par p.
5. Construction et énumération sur $\mathbb{F}_{p^2}$ en dimension quelconque.

Lemme

Soient p un nombre premier, θ l'automorphisme de Frobenius sur $\mathbb{F}_{p^2}$, $R = \mathbb{F}_{p^2}[X; \theta]$.
Soit $f(X^2)$ in $\mathbb{F}_p[X^2]$ irréductible.
Soit $h = h_1 \cdots h_k \in R$ avec h_i irréductible dans R, unitaire et divisant $f(X^2)$.
Les assertions suivantes sont équivalentes :

(i) La factorisation de h n'est pas unique.

(ii) $f(X^2)$ divise h.

(iii) Il existe i dans $\{1, \ldots, k-1\}$ tel que $h_i \cdot h_{i+1} = f(X^2)$.

Proposition

On suppose $k = p^s \times t,\ p \not| t$.

$$X^{2k} - 1 = \prod_{f_i = f_i^\natural,\ f_i\ irr} f_i(X^2)^{p^s} \prod_{f_i = g_i g_i^\natural, g_i \neq g_i^\natural\ irr} f_i(X^2)^{p^s} \in \mathbb{F}_p[X^2]$$

Le nombre de codes θ-cycliques auto-duaux sur $\mathbb{F}_{p^2}$ de dimension k est

$$N \times \prod_{f = f^\natural,\ irr, deg > 1} \frac{p^{\delta(p^s+1)} - 1}{p^\delta - 1} \times \prod_{f = gg^\natural} \frac{\left(p^{\delta(p^s+1)} - 2p^s - 3\right)\left(1 + p^\delta\right) + 4p^s + 4}{\left(p^\delta - 1\right)^2}$$

avec $\delta := \deg_{X^2}(f(X^2))/2$ et

$$N = \begin{cases} 1 & \text{si} \quad s = 0, p = 2 \\ 3 & \text{si} \quad s > 0, p = 2 \\ 2\dfrac{p^{(p^s+1)/2} - 1}{p - 1} & \text{si} \quad p \equiv 3 \pmod 4 \text{ et } k \equiv 1 \pmod 2 \\ 0 & \text{sinon.} \end{cases}$$

$$\boxed{C = C^{\perp}}$$

$$h^{\natural} \cdot h = X^n - 1$$

$\boxed{\text{longueur } n \text{ fixée}}$ $\longleftrightarrow$ système polynomial

$\boxed{\text{longueur } n \text{ et } f_i(X^2)}$ $\longleftrightarrow$ $h = \mathrm{lcrm}(h_i)$

$$h_i^{\natural} \cdot h_i = f_i(X^2)^{p^s}$$

$\boxed{C = C^{\perp}}$

$\boxed{C \cap C^{\perp} = \{0\}}$

$h^{\natural} \cdot h = X^n - 1$

$\boxed{\text{longueur } n \text{ fixée}}$ $\longleftrightarrow$ système polynomial

$\boxed{\text{longueur } n \text{ et } f_i(X^2)}$ $\longleftrightarrow$ $h = \mathrm{lcrm}(h_i)$

$h_i^{\natural} \cdot h_i = f_i(X^2)^{p^s}$

$\boxed{C = C^{\perp}}$

$g \cdot h = X^n - 1, g = h^{\natural}$

longueur n fixée

système polynomial

longueur n et $f_i(X^2)$

$g = \mathrm{lclm}(g_i), g_i h_i = f_i(X^2)^{p^s}$

$g_i = h_i^{\natural}$

$\boxed{C \cap C^{\perp} = \{0\}}$

$\mathrm{gcrd}(g, h^{\natural}) = 1$

$\boxed{C = C^{\perp}}$

$g \cdot h = X^n - 1, g = h^{\natural}$

$\boxed{C \cap C^{\perp} = \{0\}}$

$\mathrm{gcrd}(g, h^{\natural}) = 1$

longueur n fixée

longueur n et $f_i(X^2)$

système polynomial

$g = \mathrm{lclm}(g_i), g_i h_i = f_i(X^2)^{p^s}$

$g_i = h_i^{\natural}$

$\mathrm{gcrd}(g_i, h_i^{\natural}) = 1$

Troisième partie III

Codes d'évaluation tordue.

6. Evaluation des polynômes tordus (d'après Lam & Leroy, 1988).

7. Code d'évaluation tordue.

8. Décodage.

Evaluation

Pour f dans R et α dans K il existe un unique q dans R et un unique a dans K tels que $f = q \cdot (X - \alpha) + a$. L'application $f : \begin{cases} K & \to & K \\ \alpha & \mapsto & a \end{cases}$ est associée à cette division à droite et on note $a = f(\alpha)$.

Si $f = \sum a_i X^i$ alors

$$f(\alpha) = \sum a_i N_i(\alpha)$$

où $N_i(\alpha)$ est définie par :

$$N_i(x) := x\theta(x) \cdots \theta^{i-1}(x)$$

θ-classes de conjugaison

Soient $a, b \in K$, a et b sont θ-conjugués s'il existe y dans K^* tel que $b = a^y$ où

$$a^y = \theta(y)ay^{-1}$$

Ceci définit une relation d'équivalence sur K.

- Sur $K = \mathbb{F}_{2^m}$, avec $\theta : x \mapsto x^2$, il y a deux θ-classes de conjugaison :

$$\{0\} \text{ et } K^*.$$

- Sur $K = \mathbb{F}_{3^m}$, avec $\theta : x \mapsto x^3$, il y a trois θ-classes de conjugaison :

$$\{0\}, \{\theta(y)y^{-1} = y^2, y \in K^*\} \text{ et } \{\alpha\theta(y)y^{-1} = \alpha y^2, y \in K^*\}$$

où $\alpha \in K$ est générateur de K^*.

Formule du produit

Soient f et g dans R et soit α dans K.

- Si $g(\alpha) = 0$ alors $(f \cdot g)(\alpha) = 0$.
- Si $g(\alpha) \neq 0$, alors
$$(f \cdot g)(\alpha) = f(\alpha^{g(\alpha)})g(\alpha)$$

Démonstration.

$g(X) = q_1(X) \cdot (X - \alpha) + g(\alpha)$ et $f(X) = q_2(X) \cdot (X - \alpha^{g(\alpha)}) + f(\alpha^{g(\alpha)})$

$$\begin{aligned} f(X) \cdot g(X) &= f(X) \cdot q_1(X) \cdot (X - \alpha) + q_2(X) \cdot \underbrace{(X - \alpha^{g(\alpha)}) \cdot g(\alpha)}_{\theta(g(\alpha)) \cdot (X - \alpha)} \\ &\quad + f(\alpha^{g(\alpha)})g(\alpha) \\ &= (f(X) \cdot q_1(X) + q_2(X) \cdot \theta(g(\alpha))) \cdot (X - \alpha) \\ &\quad + f(\alpha^{g(\alpha)})g(\alpha) \end{aligned}$$

$\square$

Soit $n \in \mathbb{N}^*$. Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in K^n$.

P-indépendance

On dit que $\alpha_1, \ldots, \alpha_n$ sont P-indépendants si

$$\deg(\mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)) = n.$$

Matrice de Vandermonde ($k \leq n$)

$$V_{k,n}^{\theta}(\underline{\alpha}) = \begin{pmatrix} 1 & 1 & \cdots & \cdots & 1 \\ N_1(\alpha_1) & N_1(\alpha_2) & \cdots & \cdots & N_1(\alpha_n) \\ N_2(\alpha_1) & N_2(\alpha_2) & \cdots & \cdots & N_2(\alpha_n) \\ \vdots & \vdots & & & \vdots \\ N_{k-1}(\alpha_1) & N_{k-1}(\alpha_2) & \cdots & \cdots & N_{k-1}(\alpha_n) \end{pmatrix}$$

Propriété

$\mathrm{rang}(V_{n,n}^{\theta}(\underline{\alpha})) = \deg(\mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i))$

Les résultats qui précèdent se déclinent dans un contexte plus général :

- K corps non nécessairement commutatif (« division ring » ou « skew field »),
- $\theta \in End(K)$,
- δ : θ-dérivation : $\forall a, b \in K$,

$$\begin{aligned} \delta(a+b) &= \delta(a) + \delta(b) \\ \delta(ab) &= \delta(a)b + \theta(a)\delta(b) \end{aligned}$$

- $R = K[X; \theta, \delta]$, anneau de polynômes tordus :

$$\forall a \in K, X \cdot a = \theta(a)X + \delta(a)$$

- R euclidien à droite (existence de lclm, gcrd)

Si $K = \mathbb{F}_q$, alors la seule dérivation possible est $\delta = \beta(\theta - id)$ où $\beta \in \mathbb{F}_q$.
Par un changement de variable, on peut se ramener à $\delta = 0$.

$$\mathcal{H} : \left\{ \begin{array}{ccc} K[X;\theta,\delta] & \to & K[Z;\theta] \\ X & \mapsto & Z - \beta \end{array} \right. \quad \text{isomorphisme d'anneaux (Hilbert twist)}$$

$$\begin{array}{rcl} \mathcal{H}(\mathbf{X} \cdot \mathbf{a}) & = & \mathcal{H}(\theta(a)X + \delta(a)) \\ & = & \theta(a)(Z - \beta) + \beta\theta(a) - \beta a \\ & = & Z \cdot a - \beta a \\ & = & \mathcal{H}(\mathbf{X}) \cdot \mathcal{H}(\mathbf{a}) \end{array}$$

On a donc $f(\alpha) = \mathcal{H}(f)(\alpha + \beta)$
$\rightarrow$ la dérivation n'apportera rien ici.

6 Evaluation des polynômes tordus (d'après Lam & Leroy, 1988).

7 Code d'évaluation tordue.

8 Décodage.

Code d'évaluation tordue

Soient $k \leq n$ dans $\mathbb{N}^*$, soient $\alpha_1, \ldots, \alpha_n$ P-indépendants dans K.
Le code d'évaluation tordue de support $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ est défini par

$$\mathcal{C}^{\theta}_{k,n}(\underline{\alpha}) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in R, \deg(f) < k\}$$

Remarques :

- $\mathcal{C}^{\theta}_{k,n}(\underline{\alpha}) = \{m \times V^{\theta}_{k,n}(\underline{\alpha}) \mid m \in \mathbb{F}_q^k\}$
- $\mathcal{C}^{\theta}_{k,n}(\underline{\alpha})$ est de dimension k.

Proposition

Soit $k \leq n \in \mathbb{N}^*$. Soient $\alpha_1, \ldots, \alpha_n$ P-indépendants dans $\mathbb{F}_q$.
$\mathcal{C}^{\theta}_{k,n}(\underline{\alpha})$ est un code MDS $(d = n - k + 1)$.

Démonstration.

On montre que le code ne possède pas de mot non nul de poids $< n - k + 1$.

Soit $c = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $\deg(f) < k$ et $w_H(c) \leq n - k$.

Soit $I = \{i \in \{1, \ldots, n\} \mid f(\alpha_i) = 0\}$ et soit $S(X) = \mathrm{lclm}_{i \in I}(X - \alpha_i)$.

Alors $\#I \geq k$, $\deg(S) = \#I$ car $(\alpha_i)_{i \in I}$ sont P-indépendants et $S(X)$ divise $f(X)$ à droite ;

donc $f = 0$ et $c = 0$.

□

Exemples

- $K = \mathbb{F}_q$, $\theta = id$, $\alpha_1, \dots, \alpha_n$ distincts deux à deux :

  code GRS (Generalized Reed Solomon)

- $K = \mathbb{F}_q$, $\theta = id$, $\alpha_i = \alpha^{i-1}$ avec α racine primitive n^e de 1 :

  code RS (Reed Solomon)

- $K = \mathbb{F}_q = \mathbb{F}_{p^m}$, $\theta : x \mapsto x^p$,
  $\alpha_1, \ldots, \alpha_n$ P-indépendants et conjugués à 1 $(\forall i, \alpha_i = \theta(y_i)/y_i)$:
  code équivalent à un code de Gabidulin de support $(y_1, \ldots, y_n)$.

$$V_{k,n}^{\theta}(\underline{\alpha}) = \begin{pmatrix} y_1 & y_2 & \cdots & \cdots & y_n \\ \theta(y_1) & \theta(y_2) & \cdots & \cdots & \theta(y_n) \\ \vdots & \vdots & & & \vdots \\ \theta^{k-1}(y_1) & \theta^{k-1}(y_2) & \cdots & \cdots & \theta^{k-1}(y_n) \end{pmatrix} \times$$

$$\begin{pmatrix} 1/y_1 & 0 & \cdots & \cdots & 0 \\ 0 & 1/y_2 & \cdots & \cdots & 0 \\ \vdots & & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & \cdots & 1/y_n \end{pmatrix}$$

Soit C un code $[n, k, d]_q$.
Soit τ un entier, soit $c \in C$. Soit $r = c + e$ avec $w_H(e) \leq \tau$.
On veut déterminer

$$\mathcal{D}(r) = \{\tilde{c} \in C \mid w_H(\tilde{c} - r) \leq \tau\}$$

c'est à dire l'ensemble des $\tilde{c}$ de C tels que $\tilde{c}_i = r_i$ pour au moins $n - \tau$ valeurs de i.

Soit $t = \lfloor \frac{d-1}{2} \rfloor$ (capacité de correction du code).

Si $\tau \leq t$, on a un *décodage unique* ($\mathcal{D}(r) = \{c\}$),
sinon on parle de *décodage en liste*.

Ici $d = n - k + 1$ (code MDS) et $c = (f(\alpha_1), \ldots, f(\alpha_n))$ avec $f \in R_{<k}$.

On veut trouver tous les polynômes g de degré $< k$ tels que $g(\alpha_i) = r_i$ pour au moins $n - \tau$ valeurs de i

$\rightarrow$ problème de ≪ reconstruction polynomiale ≫

- Cas commutatif (code RS/GRS) :
  Berlekamp Welch (1960) pour le décodage unique ;
  Sudan (1999) et Guruswami (2002) pour le décodage en liste.
- Cas des codes de Gabidulin :
  Loidreau (2007) et Robert (2016) pour le décodage unique avec la métrique rang.

Principe du décodage (Berlekamp-Welch)

[D. Augot, JNCF 2010, chap.4]

C, code GRS $[n, k, n-k+1]_q$ de support $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n$ distincts deux à deux.

$c = (f(\alpha_1), \dots, f(\alpha_n)) \in C$, $r = c + e$ avec $w_H(e) \leq t := \lfloor (n-k)/2 \rfloor$.

- Soit $E(X) = \prod_{i \mid e_i \neq 0} (X - \alpha_i)$ (polynôme localisateur d'erreurs). Alors

$$\forall i \in \{1, \dots, n\}, f(\alpha_i) = r_i \text{ ou } E(\alpha_i) = 0$$

donc $E(f - r_i) = Ef - Er_i$ s'annule en α_i pour tout i :

$$(Ef)(\alpha_i) - E(\alpha_i) r_i = 0$$

De plus $\deg(E) \leq t$ et $\deg(f) \leq k-1$

- Soient $Q_0(X)$ et $Q_1(X) \in \mathbb{F}_q[X]$ sont tels que $Q_0 + Q_1 r_i$ s'annule en α_i pour tout i de $\{1, \ldots, n\}$:

$$(*)\ Q_0(\alpha_i) + Q_1(\alpha_i) r_i = 0$$

avec $\deg(Q_1) \leq t$ et $\deg(Q_0) \leq t + k - 1$, alors $f = -Q_0/Q_1$.

En effet

> $Q_0 + Q_1 f$ *s'annule en au moins* $n - t$ *points distincts ;*
> $\deg(Q_0 + Q_1 f) \leq t + k - 1 \leq n - t - 1$

donc $Q_0 + Q_1 f = 0$.

Remarque : nombre d'inconnues : $(t+1) + (t+k) \geq n+1$ donc $(*)$ a une solution.

C un code d'évaluation tordue $[n, k, n-k+1]_q$ de support $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ avec $\alpha_1, \dots, \alpha_n$ P-indépendants.

$c = (f(\alpha_1), \dots, f(\alpha_n)) \in C$, $r = c + e$ avec $w_H(e) \leq t := \lfloor (n-k)/2 \rfloor$.

- Soit $E(X) = \mathrm{lclm}_{i | e_i \neq 0}(X - \alpha_i^{e_i})$ (polynôme tordu localisateur d'erreurs). Alors

$$\forall i \in \{1, \dots, n\}, f(\alpha_i) = r_i \text{ ou } E(\alpha_i^{f(\alpha_i) - r_i}) = 0$$

donc $E \cdot (f - r_i) = E \cdot f - E \cdot r_i$ s'annule en α_i pour tout i :

$$\begin{cases} (E \cdot f)(\alpha_i) - E(\alpha_i^{r_i}) r_i = 0 & \text{si } r_i \neq 0 \\ (E \cdot f)(\alpha_i) = 0 & \text{si } r_i = 0 \end{cases}$$

- Soient $Q_0(X)$ et $Q_1(X) \in R$ sont tels que pour tout i, $Q_0 + Q_1 \cdot r_i$ s'annule en α_i :

$$(*) \begin{cases} Q_0(\alpha_i) + Q_1(\alpha_i^{r_i})r_i = 0 & \text{si } r_i \neq 0 \\ Q_0(\alpha_i) = 0 & \text{si } r_i = 0 \end{cases}$$

avec $\deg(Q_1) \leq t$ et $\deg(Q_0) \leq k-1$, alors f est le reste de la division à droite de $-Q_0$ par Q_1.

En effet

$(Q_0 + Q_1 \cdot f)(\alpha_i) = 0$ *si* $r_i = f(\alpha_i)$ *i.e.* $e_i = 0$;
$\mathrm{lclm}_{i|e_i=0}(X - \alpha_i)$ *divise* $Q_0 + Q_1 \cdot f$ *à droite* ;
$\deg \mathrm{lclm}_{i|e_i=0}(X - \alpha_i) \geq n - t$ *car les* α_i *sont* P*-indépendants* ;
$\deg(Q_0 + Q_1 f) \leq t + k - 1 \leq n - t - 1$;

donc $Q_0 + Q_1 \cdot f = 0$.

Algorithme

Entrée : $r = c + e$ avec $c = (f(\alpha_1), \ldots, f(\alpha_n))$, $f \in \mathbb{F}_q[X;\theta]$, $\deg(f) < k$, $e \in \mathbb{F}_q^n$ et $\mathrm{w_H}(e) \leq t = (n-k-1)/2$

Sortie : f

1 : Trouver Q_0 de degré $\leq k+t$, Q_1 de degré $\leq t$ tels que pour tout i dans $\{1, \ldots, n\}$

$$(*) \begin{cases} Q_0(\alpha_i) + Q_1(\alpha_i^{r_i})r_i = 0 & \text{si } r_i \neq 0 \\ Q_0(\alpha_i) = 0 & \text{si } r_i = 0 \end{cases}$$

2 : $f(X) \leftarrow$ quotient dans la division à gauche de $Q_0(X)$ par $-Q_1(X)$ dans $\mathbb{F}_q[X;\theta]$

3 : **rendre** f

Une observation ...

- Dans le cas commutatif,

$$E(X) = \prod_{e_i \neq 0} (X - \alpha_i)$$

a un degré égal au poids $w_H(e)$ de e.

- Dans le cas non commutatif,

$$E(X) = \mathrm{lclm}_{e_i \neq 0}(X - \alpha_i^{e_i})$$

a un degré inférieur ou égal à $w_H(e)$ (car les $\alpha_i^{e_i}$ ne sont pas nécessairement P-indépendants).

... une nouvelle métrique.

Considérons

$$w_{\underline{\alpha}}(e) = \begin{cases} \deg \operatorname{lclm}_{e_i \neq 0}(X - \alpha_i^{e_i}) & \text{si } e \neq 0 \\ 0 & \text{sinon} \end{cases}$$

+ On montre que $w_{\underline{\alpha}}$ est le poids de la métrique tordue définie dans [U. Martínez-Peñas, 2018]
+ Avec cette métrique, les codes d'évaluation tordue sont MDS.
+ L'algorithme de décodage précédent reste valide.

Merci pour votre attention !