Codes linéaires à base de polynômes tordus avec automorphismes et dérivations

D. Boucher, F. Ulmer
IRMAR, Université Rennes 1

Séminaire Algorithmes, INRIA Rocquencourt, 13 février 2012

Definition (codes θ-cycliques, 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 $\theta : x \mapsto x^q$, alors C est un code q-cyclique de Gabidulin (1985).

$R = F[X;\theta]$, $\theta \in Aut(F)$, $\boxed{X \cdot a = \theta(a)X}$

(Ore, 1933)

$$
\begin{array}{ccccc}
R/R(X^n-1) & & R\text{-module à gauche} & \leftrightarrow & F^n \\
\cup & & & & \cup \\
Rg/R(X^n-1) & & R\text{-sous-module à gauche} & \leftrightarrow & \text{code } \theta\text{-cyclique} \\
\updownarrow & & & & \\
g|_d X^n-1 & & & &
\end{array}
$$

$$R = F[X;\theta], \ \theta \in Aut(F), \quad \boxed{X \cdot a = \theta(a)X}$$

$$\begin{array}{ccccc} R/Rf, \deg(f) = n & & R\text{-module à gauche} & \leftrightarrow & F^n \\ \cup & & & & \cup \\ Rg/Rf & & R\text{-sous-module à gauche} & \leftrightarrow & \theta\text{-code module} \\ \updownarrow & & & & \\ g|_d f & & & & \end{array}$$

$R = F[X; \theta, \delta]$, $\theta \in Aut(F)$, $\delta = \beta(\theta - id), \beta \in F$, $\boxed{X \cdot a = \theta(a)X + \delta(a)}$

$$
\begin{array}{ccccc}
R/Rf, \deg(f) = n & & R\text{-module à gauche} & \leftrightarrow & F^n \\
\cup & & & & \cup \\
Rg/Rf & & R\text{-sous-module à gauche} & \leftrightarrow & (\theta, \delta)\text{-code module} \\
\updownarrow & & & & \\
g|_d f & & & &
\end{array}
$$

Definition ((θ, δ)-codes modules)

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

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

Notation : $(g)_n^{\theta,\delta}$

Remarque

Si $\delta = 0$, on a un θ-code module et deux cas sont possibles :

- $\exists a \in F, g|_d X^n - a$, alors C est θ-constacyclique.
- $\forall a \in F, g \not|_d X^n - a$, alors C est θ-cyclique raccourci.

Question

Les familles des θ-codes modules et des (θ, δ)-codes modules sont-elles distinctes ?

Definition ((θ, δ)-codes modules)

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

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

Notation : $(g)_n^{\theta,\delta}$

Remarque

Si $\delta = 0$, on a un θ-code module et deux cas sont possibles :

- $\exists a \in F, g|_d X^n - a$, alors C est θ-constacyclique.
- $\forall a \in F, g \not|_d X^n - a$, alors C est θ-cyclique raccourci.

Question

Les familles des θ-codes modules et des (θ, δ)-codes modules sont-elles distinctes ?

Hilbert twist

Il y a un isomorphisme d'anneaux entre $F[X;\theta,\delta]$ et $F[Z;\theta]$ défini par

$$\mathcal{H}: \begin{cases} F[X;\theta,\delta] & \to & F[Z;\theta] \\ X & \mapsto & Z-\beta \\ X^i & \mapsto & (Z-\beta)^i = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) Z^j \\ \\ c=(c_0,\ldots,c_{n-1}) & \mapsto & c \times A_n(\beta) \end{cases}$$

avec $A_n(\beta) = (a_{i+1,j+1}(\beta))$ matrice carrée triangulaire inférieure inversible (avec diagonale unité).

On a bien, pour a dans F,

$$\mathcal{H}(\mathbf{X}\cdot\mathbf{a}) = \mathcal{H}(\theta(a)X+\delta(a)) = \theta(a)(Z-\beta)+\delta(a) = Z\cdot a - \beta a = \mathcal{H}(\mathbf{X})\cdot\mathcal{H}(\mathbf{a})$$

Matrice génératrice

- Si $\delta = 0$, une matrice génératrice de $(g)_n^\theta$ est

$$G_{g,n}^\theta = \begin{pmatrix} g_0 & \dots & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \dots & \theta(g_{n-k}) & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & \theta^{k-1}(g_0) & \dots & \dots & \theta^{k-1}(g_{n-k}) \end{pmatrix}$$

- Si $\delta \neq 0$, une matrice génératrice de $(g)_n^{\theta,\delta}$ est

$$G_{g,n}^{\theta,\delta} = A_k(\beta) \times G_{\mathcal{H}(g),n}^\theta \times A_n(\beta)^{-1}$$

Démonstration.

$$\begin{aligned} c \in (g)_n^{\theta,\delta} &\Leftrightarrow c(X) = m(X) \cdot g(X) && \in F[X;\theta,\delta] \\ &\Leftrightarrow \mathcal{H}(c(X)) = \mathcal{H}(m(X)) \cdot \mathcal{H}(g(X)) && \in F[Z;\theta] \\ &\Leftrightarrow (c \times A_n(\beta)) = (m \times A_k(\beta)) \times G_{\mathcal{H}(g),n}^\theta \end{aligned}$$

Matrice génératrice

- Si $\delta = 0$, une matrice génératrice de $(g)_n^\theta$ est

$$G_{g,n}^\theta = \begin{pmatrix} g_0 & \dots & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & \theta(g_0) & \dots & \dots & \theta(g_{n-k}) & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & \theta^{k-1}(g_0) & \dots & \dots & \theta^{k-1}(g_{n-k}) \end{pmatrix}$$

- Si $\delta \neq 0$, une matrice génératrice de $(g)_n^{\theta,\delta}$ est

$$G_{g,n}^{\theta,\delta} = A_k(\beta) \times G_{\mathcal{H}(g),n}^\theta \times A_n(\beta)^{-1}$$

Démonstration.

$$\begin{aligned} c \in (g)_n^{\theta,\delta} \quad &\Leftrightarrow \quad c(X) = m(X) \cdot g(X) && \in F[X;\theta,\delta] \\ &\Leftrightarrow \quad \mathcal{H}(c(X)) = \mathcal{H}(m(X)) \cdot \mathcal{H}(g(X)) && \in F[Z;\theta] \\ &\Leftrightarrow \quad (c \times A_n(\beta)) = (m \times A_k(\beta)) \times G_{\mathcal{H}(g),n}^\theta \end{aligned}$$

□

Exemple sur $\mathbb{F}_4 = \mathbb{F}_2(a)$, $\theta : x \mapsto x^2$ et $\delta : x \mapsto a(\theta(x) - x)$

- $g = X^2 + X + a^2 \in \mathbb{F}_4[X; \theta, \delta] \to \mathcal{H}(g) = Z^2 + a \in \mathbb{F}_4[Z; \theta]$ avec

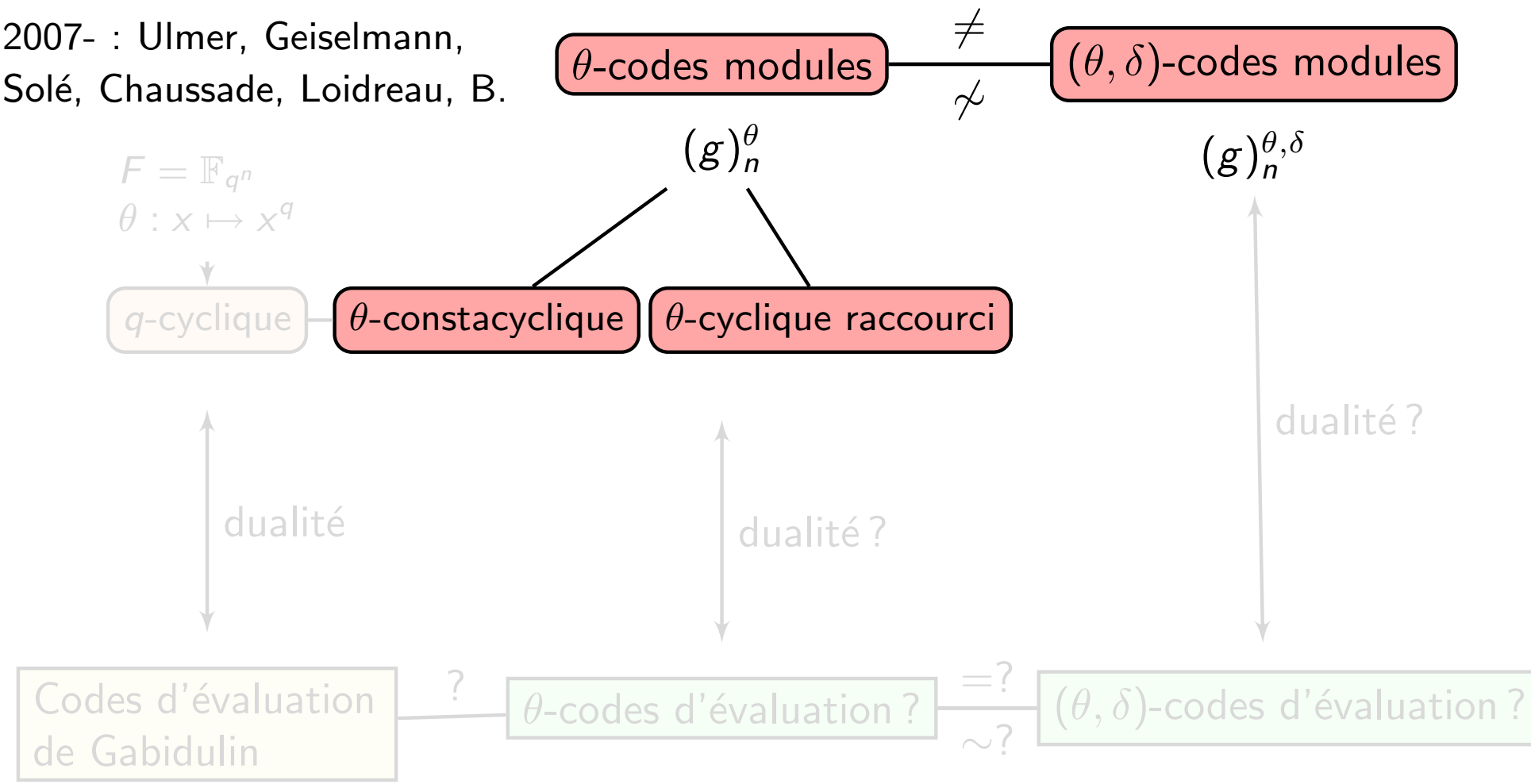
$$\begin{array}{rccc} \mathcal{H} : & \mathbb{F}_4[X; \theta, \delta] & \to & \mathbb{F}_4[Z; \theta] \\ & X & \mapsto & Z - a \\ & X^2 & \mapsto & Z^2 + Z + a^2 \end{array}$$

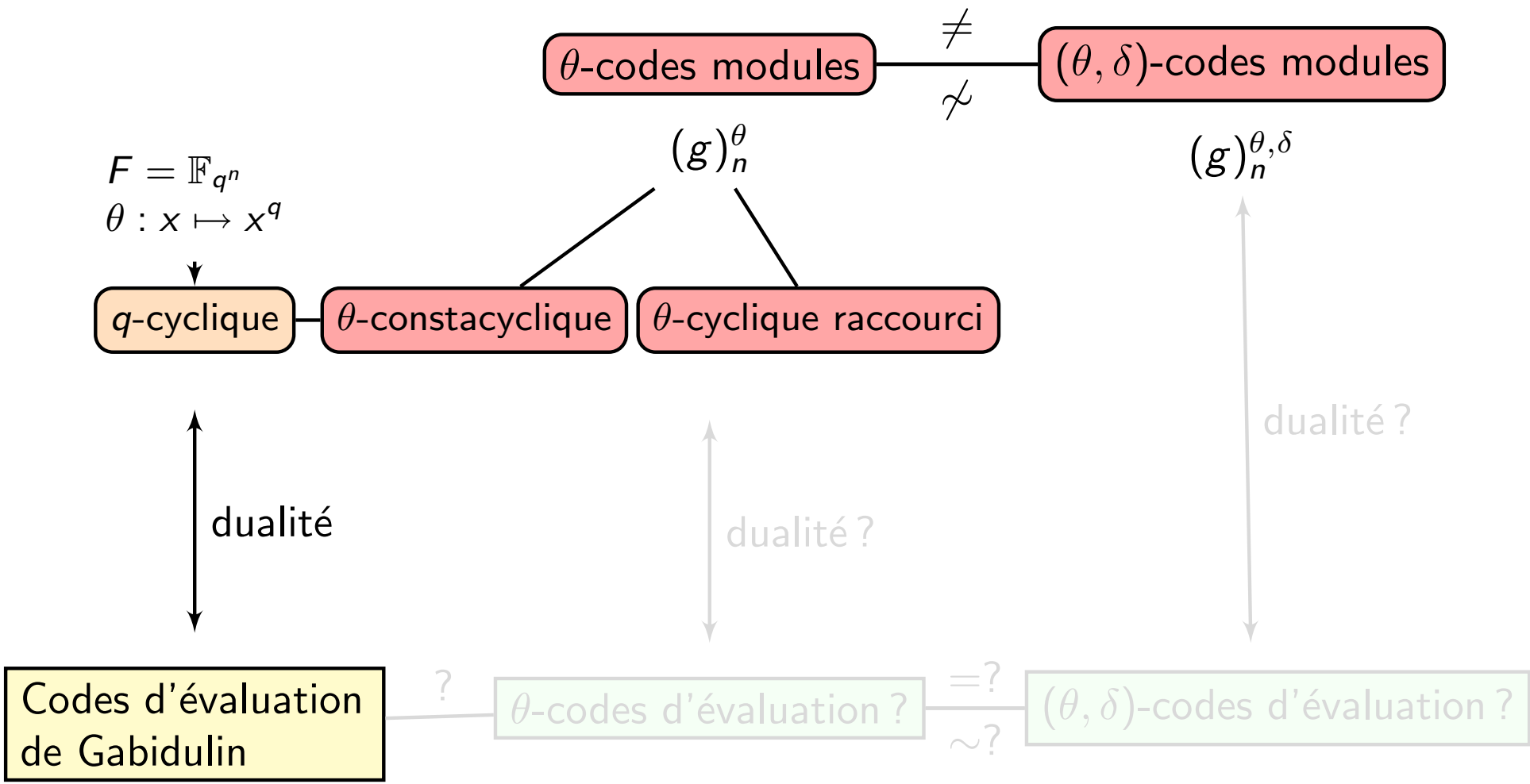
$$G_{g,5}^{\theta,\delta} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ a^2 & 1 & 1 \end{pmatrix}}_{A_3(a)} \times \underbrace{\begin{pmatrix} a & 0 & 1 & 0 & 0 \\ 0 & a^2 & 0 & 1 & 0 \\ 0 & 0 & a & 0 & 1 \end{pmatrix}}_{G^{\theta}_{\mathcal{H}(g),5}} \times \underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ a & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ a & a^2 & a^2 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}}_{A_5(a)^{-1}}$$

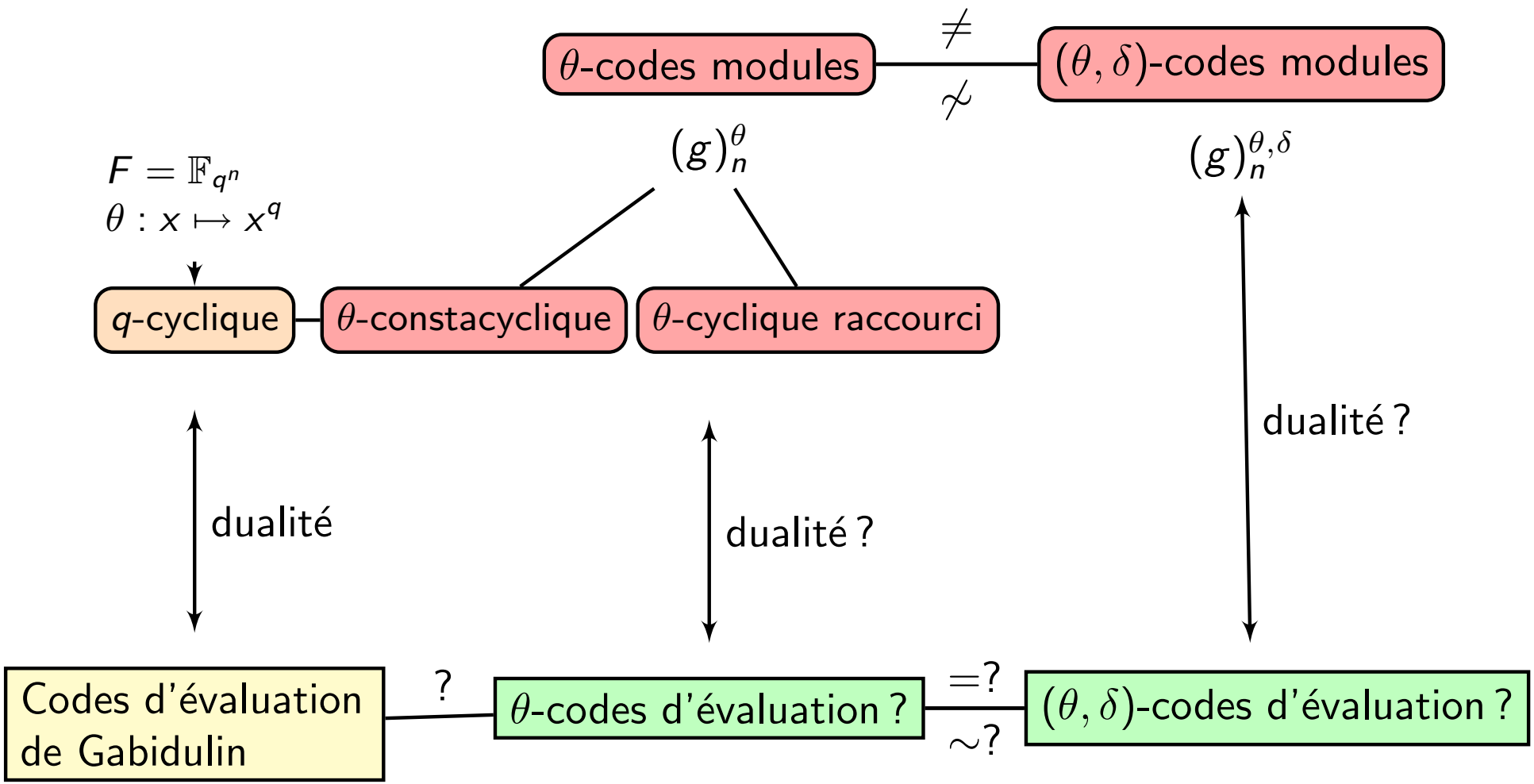
$$= \begin{pmatrix} a^2 & 1 & 1 & 0 & 0 \\ a & a & 1 & 1 & 0 \\ a & 1 & a^2 & 1 & 1 \end{pmatrix}$$

- $(g)_5^{\theta,\delta}$: (θ, δ)-code module $[5, 3, \mathbf{3}]_4$ mais $(\mathcal{H}(g))_5^{\theta}$: θ-code module $[5, 3, \mathbf{2}]_4$.
- Il n'existe pas de θ-code module $[5, 3, 3]_4$.

2007- : Ulmer, Geiselmann, Solé, Chaussade, Loidreau, B.




θ-codes modules
$\neq$
$\not\sim$
(θ, δ)-codes modules
$(g)_n^{\theta}$
$(g)_n^{\theta,\delta}$
$F = \mathbb{F}_{q^n}$
$\theta : x \mapsto x^q$
q-cyclique
θ-constacyclique
θ-cyclique raccourci
dualité
dualité ?
dualité ?
Codes d'évaluation de Gabidulin
?
θ-codes d'évaluation ?
$=?$
$\sim?$
(θ, δ)-codes d'évaluation ?


θ-codes modules
$\neq$
$\not\sim$
(θ, δ)-codes modules
$(g)_n^{\theta}$
$(g)_n^{\theta,\delta}$
$F = \mathbb{F}_{q^n}$
$\theta : x \mapsto x^q$
q-cyclique
θ-constacyclique
θ-cyclique raccourci
dualité
dualité ?
dualité ?
Codes d'évaluation de Gabidulin
?
θ-codes d'évaluation ?
$=?$
$\sim?$
(θ, δ)-codes d'évaluation ?

1. (θ, δ)-codes modules

2. (θ, δ)-codes d'évaluation
   - Définitions et comparaisons
   - Dualité et sous-familles

3. Un algorithme de décodage

4. Conclusion et perspectives

But :

- Définir deux familles de (θ, δ)-*codes d'évaluation* et les *comparer* (égalité, équivalence).

$\longrightarrow$ outil principal : *Vandermonde and Wronskian Matrices over Division Rings*, T.Y. Lam and A. Leroy, 1988

- Construire des *sous-familles* de (θ, δ)-codes d'évaluation dont les *duaux* forment des *sous-familles* de (θ, δ)-codes modules.

$\longrightarrow$ conséquence : familles de (θ, δ)-codes modules dont on peut prescrire la distance.

Evaluation dans $F[X;\theta,\delta]$

Soit $f = \sum_{i=0}^{d} f_i X^i \in F[X;\theta,\delta]$

- Evaluation par reste à droite : pour $\alpha \in F$,

$$f(\alpha) := \sum_{i=0}^{d} f_i \; N_i^{\theta,\delta}(\alpha)$$

où $N_0^{\theta,\delta}(\alpha) = 1$ et $\forall i \in \mathbb{N}, N_{i+1}^{\theta,\delta}(\alpha) = \theta(N_i^{\theta,\delta}(\alpha))\,\alpha + \delta(N_i^{\theta,\delta}(\alpha))$.

- Evaluation linéaire : pour $y \in F$,

$$\mathcal{L}_f(y) := \sum_{i=0}^{d} f_i \; \mathcal{D}^i(y) \text{ avec } \mathcal{D} = \begin{cases} \theta & si\ \delta = 0 \\ \delta & sinon \end{cases}$$

Proposition (Lam Leroy)

1. $\forall i \in \mathbb{N}, \forall y \in F, N_i^{\theta}(\theta(y)y^{-1}) = \theta^i(y)y^{-1}$.
2. $\forall i \in \mathbb{N}, \forall y \in F, N_i^{\theta,\delta}(\delta(y)y^{-1}) = \delta^i(y)y^{-1}$.

Evaluation dans $F[X;\theta,\delta]$

Soit $f = \sum_{i=0}^{d} f_i X^i \in F[X;\theta,\delta]$

- Evaluation par reste à droite : pour $\alpha \in F$,

$$f(\alpha) := \sum_{i=0}^{d} f_i \; N_i^{\theta,\delta}(\alpha)$$

où $N_0^{\theta,\delta}(\alpha) = 1$ et $\forall i \in \mathbb{N}, N_{i+1}^{\theta,\delta}(\alpha) = \theta(N_i^{\theta,\delta}(\alpha))\,\alpha + \delta(N_i^{\theta,\delta}(\alpha))$.

- Evaluation linéaire : pour $y \in F$,

$$\mathcal{L}_f(y) := \sum_{i=0}^{d} f_i \; \mathcal{D}^i(y) \text{ avec } \mathcal{D} = \begin{cases} \theta & si\ \delta = 0 \\ \delta & sinon \end{cases}$$

Proposition (Lam Leroy)

1. $\forall i \in \mathbb{N}, \forall y \in F, N_i^{\theta}(\theta(y)y^{-1}) = \theta^i(y)y^{-1}$.
2. $\forall i \in \mathbb{N}, \forall y \in F, N_i^{\theta,\delta}(\delta(y)y^{-1}) = \delta^i(y)y^{-1}$.

Proposition

Soit $i \in \mathbb{N}$.

1. $\forall \alpha \in F, N_i^{\theta,\delta}(\alpha) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\alpha + \beta)$
2. $\forall y \in F, \delta^i(y) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\beta) \theta^j(y)$

Démonstration.

Soit $i \in \mathbb{N}$.

1. Soit $\alpha \in F$.Soit $Q(X) \in F[X; \theta, \delta]$ tel que

$$\begin{array}{ccc} X^i & = & Q(X) \cdot (X - \alpha) + N_i^{\theta,\delta}(\alpha) \in F[X; \theta, \delta]. \\ & \downarrow \mathcal{H} & \\ \sum_{j=0}^{i} a_{i+1,j+1}(\beta) Z^j & = & \mathcal{H}(Q(X)) \cdot (Z - \beta - \alpha) + N_i^{\theta,\delta}(\alpha) \in F[Z; \theta] \end{array}$$

   donc $N_i^{\theta,\delta}(\alpha) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\alpha + \beta)$.

2. On applique la relation précédente à $\alpha = \delta(y) y^{-1}$.

□

Proposition

Soit $i \in \mathbb{N}$.

1. $\forall \alpha \in F, N_i^{\theta,\delta}(\alpha) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\alpha + \beta)$
2. $\forall y \in F, \delta^i(y) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\beta) \theta^j(y)$

Démonstration.

Soit $i \in \mathbb{N}$.

1. Soit $\alpha \in F$.Soit $Q(X) \in F[X; \theta, \delta]$ tel que

$$\begin{array}{ccc} X^i & = & Q(X) \cdot (X - \alpha) + N_i^{\theta,\delta}(\alpha) \in F[X; \theta, \delta]. \\ & \downarrow \mathcal{H} & \\ \sum_{j=0}^{i} a_{i+1,j+1}(\beta) Z^j & = & \mathcal{H}(Q(X)) \cdot (Z - \beta - \alpha) + N_i^{\theta,\delta}(\alpha) \in F[Z; \theta] \end{array}$$

   donc $N_i^{\theta,\delta}(\alpha) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\alpha + \beta)$.

2. On applique la relation précédente à $\alpha = \delta(y) y^{-1}$.

□

Matrice de Vandermonde

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

$$V_{k,n}^{\theta,\delta}(\underline{\alpha}) = \left(N_{i-1}^{\theta,\delta}(\alpha_j)\right)_{1 \leq i \leq k, 1 \leq j \leq n}$$

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

Propriété (Lam Leroy)

- $\operatorname{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = \deg(\underbrace{\operatorname{lclm}_{1 \leq i \leq n}(X - \alpha_i)}_{\in F[X;\theta,\delta]})$
- $\operatorname{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n \Leftrightarrow \alpha_1, \ldots, \alpha_n$ P-indépendants.

Matrice de Vandermonde

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

$$V_{k,n}^{\theta,\delta}(\underline{\alpha}) = \left(N_{i-1}^{\theta,\delta}(\alpha_j)\right)_{1 \leq i \leq k, 1 \leq j \leq n}$$

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

Propriété (Lam Leroy)

- $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = \deg(\underbrace{\mathrm{lclm}_{1 \leq i \leq n}(X - \alpha_i)}_{\in F[X;\theta,\delta]})$
- $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n \Leftrightarrow \alpha_1, \ldots, \alpha_n$ P-indépendants.

Wronskien

Soient $k, n \in \mathbb{N}^*$.
Soit $\underline{y} = (y_1, \ldots, y_n) \in F^n$.

$$Wr_{k,n}^{\theta,\delta}(\underline{y}) = \left(\mathcal{D}^{i-1}(y_j)\right)_{1 \leq i \leq k, 1 \leq j \leq n}$$

$$Wr_{k,n}^{\theta,\delta}(\underline{y}) = \begin{pmatrix} y_1 & y_2 & \cdots & \cdots & y_n \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \cdots & \mathcal{D}(y_n) \\ \mathcal{D}^2(y_1) & \mathcal{D}^2(y_2) & \cdots & \cdots & \mathcal{D}^2(y_n) \\ \vdots & \vdots & & & \vdots \\ \mathcal{D}^{k-1}(y_1) & \mathcal{D}^{k-1}(y_2) & \cdots & \cdots & \mathcal{D}^{k-1}(y_n) \end{pmatrix}$$

Propriété (Lam Leroy)

- $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = \mathrm{rang}(Wr_n^{\theta}(\underline{y})) = \dim_{F^\theta}(Vect(y_1, \ldots, y_n))$.
- $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n \Leftrightarrow y_1, \ldots, y_n$ linéairement indépendants sur F^θ.

Wronskien

Soient $k, n \in \mathbb{N}^*$.
Soit $\underline{y} = (y_1, \ldots, y_n) \in F^n$.

$$Wr_{k,n}^{\theta,\delta}(\underline{y}) = \left(\mathcal{D}^{i-1}(y_j)\right)_{1 \leq i \leq k, 1 \leq j \leq n}$$

$$Wr_{k,n}^{\theta,\delta}(\underline{y}) = \begin{pmatrix} y_1 & y_2 & \cdots & \cdots & y_n \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \cdots & \mathcal{D}(y_n) \\ \mathcal{D}^2(y_1) & \mathcal{D}^2(y_2) & \cdots & \cdots & \mathcal{D}^2(y_n) \\ \vdots & \vdots & & & \vdots \\ \mathcal{D}^{k-1}(y_1) & \mathcal{D}^{k-1}(y_2) & \cdots & \cdots & \mathcal{D}^{k-1}(y_n) \end{pmatrix}$$

Propriété (Lam Leroy)

- $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = \mathrm{rang}(Wr_n^{\theta}(\underline{y})) = \dim_{F^\theta}(Vect(y_1, \ldots, y_n))$.
- $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n \Leftrightarrow y_1, \ldots, y_n$ linéairement indépendants sur F^θ.

(θ,δ)-codes d'évaluation

Soient $k \leq n \in \mathbb{N}^*$.

- Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in F^n$ tel que $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n$.
  Le (θ,δ)-code d'évaluation par restes à droite de support $\underline{\alpha}$, longueur n et dimension k est défini par :

$$\mathcal{R}_{k,n}^{\theta,\delta}(\underline{\alpha}) := \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in F[X;\theta,\delta], \deg(f) < k\}$$

- Soit $\underline{y} = (y_1, \ldots, y_n) \in F^n$ tel que $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n$.
  Le (θ,δ)-code d'évaluation linéaire de support $\underline{y}$, longueur n et dimension k est défini par :

$$\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y}) := \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in F[X;\theta,\delta], \deg(f) < k\}$$

Si $\delta = 0$, $F = \mathbb{F}_{q^n}$ et $\theta : x \mapsto x^q$, alors $\mathcal{O}_{k,n}^{\theta}(\underline{y})$ est un code de Gabidulin !

Matrices génératrices

Soient $k \leq n \in \mathbb{N}^*$.

- Soit $\underline{\alpha} \in F^n$ tel que $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n$.
  Une matrice génératrice de $\mathcal{R}_{k,n}^{\theta,\delta}(\underline{\alpha})$ est $V_{k,n}^{\theta,\delta}(\underline{\alpha})$.
- Soit $\underline{y} \in F^n$ tel que $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n$.
  Une matrice génératrice de $\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y})$ est $Wr_{k,n}^{\theta,\delta}(\underline{y})$.

Démonstration.

- $\forall j \in \{1, \ldots, n\}, f(\alpha_j) = \sum_{i=1}^{k} f_{i-1} N_{i-1}^{\theta,\delta}(\alpha_j)$ donc

$$(f(\alpha_1), \ldots, f(\alpha_n)) = (f_0, \ldots, f_{k-1}) \times V_{k,n}^{\theta,\delta}(\underline{\alpha}).$$

- $\forall j \in \{1, \ldots, n\}, \mathcal{L}_f(y_j) = \sum_{i=1}^{k} f_{i-1} \mathcal{D}^{i-1}(y_j)$ donc

$$(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) = (f_0, \ldots, f_{k-1}) \times Wr_{k,n}^{\theta,\delta}(\underline{y}).$$

□

Matrices génératrices

Soient $k \leq n \in \mathbb{N}^*$.

- Soit $\underline{\alpha} \in F^n$ tel que $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n$.
  Une matrice génératrice de $\mathcal{R}_{k,n}^{\theta,\delta}(\underline{\alpha})$ est $V_{k,n}^{\theta,\delta}(\underline{\alpha})$.
- Soit $\underline{y} \in F^n$ tel que $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n$.
  Une matrice génératrice de $\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y})$ est $Wr_{k,n}^{\theta,\delta}(\underline{y})$.

Démonstration.

- $\forall j \in \{1, \ldots, n\}, f(\alpha_j) = \sum_{i=1}^{k} f_{i-1} N_{i-1}^{\theta,\delta}(\alpha_j)$ donc

$$(f(\alpha_1), \ldots, f(\alpha_n)) = (f_0, \ldots, f_{k-1}) \times V_{k,n}^{\theta,\delta}(\underline{\alpha}).$$

- $\forall j \in \{1, \ldots, n\}, \mathcal{L}_f(y_j) = \sum_{i=1}^{k} f_{i-1} \mathcal{D}^{i-1}(y_j)$ donc

$$(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) = (f_0, \ldots, f_{k-1}) \times Wr_{k,n}^{\theta,\delta}(\underline{y}).$$

□

Proposition

1. Soit $\underline{\alpha} \in F^n$ tel que $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n$. Alors $\mathcal{R}_{k,n}^{\theta,\delta}(\underline{\alpha}) = \mathcal{R}_{k,n}^{\theta}(\underline{\alpha} + \beta)$.
2. Soit $\underline{y} \in F^n$ tel que $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n$. Alors $\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y}) = \mathcal{O}_{k,n}^{\theta}(\underline{y})$.

Démonstration.

1. $\forall \alpha \in F, \forall i \in \mathbb{N}, N_i^{\theta,\delta}(\alpha) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\alpha + \beta)$ donc

$$V_{k,n}^{\theta,\delta}(\underline{\alpha}) = A_k(\beta) \times V_{k,n}^{\theta}(\underline{\alpha} + \beta).$$

2. $\forall y \in F, \forall i \in \mathbb{N}, \delta^i(y) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\beta) \theta^j(y)$ donc

$$Wr_{k,n}^{\theta,\delta}(\underline{y}) = diag(N_j^{\theta}(\beta)) \times A_k(\beta) \times Wr_{k,n}^{\theta}(\underline{y}).$$

□

Proposition

1. Soit $\underline{\alpha} \in F^n$ tel que $\mathrm{rang}(V_n^{\theta,\delta}(\underline{\alpha})) = n$. Alors $\mathcal{R}_{k,n}^{\theta,\delta}(\underline{\alpha}) = \mathcal{R}_{k,n}^{\theta}(\underline{\alpha} + \beta)$.
2. Soit $\underline{y} \in F^n$ tel que $\mathrm{rang}(Wr_n^{\theta,\delta}(\underline{y})) = n$. Alors $\mathcal{O}_{k,n}^{\theta,\delta}(\underline{y}) = \mathcal{O}_{k,n}^{\theta}(\underline{y})$.

Démonstration.

1. $\forall \alpha \in F, \forall i \in \mathbb{N}, N_i^{\theta,\delta}(\alpha) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\alpha + \beta)$ donc

$$V_{k,n}^{\theta,\delta}(\underline{\alpha}) = A_k(\beta) \times V_{k,n}^{\theta}(\underline{\alpha} + \beta).$$

2. $\forall y \in F, \forall i \in \mathbb{N}, \delta^i(y) = \sum_{j=0}^{i} a_{i+1,j+1}(\beta) N_j^{\theta}(\beta) \theta^j(y)$ donc

$$Wr_{k,n}^{\theta,\delta}(\underline{y}) = diag(N_j^{\theta}(\beta)) \times A_k(\beta) \times Wr_{k,n}^{\theta}(\underline{y}).$$

□

θ-classes de conjugaison (Lam)

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

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

On dit encore que b est θ-conjugué à a. Ceci définit une relation d'équivalence sur F et F est partitionné en θ-classes de conjugaison.

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

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

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

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

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

Proposition

Soit $\underline{\alpha} \in F^n$ tel que $\mathrm{rang}(V_n^\theta(\underline{\alpha})) = n$.
Si les α_i sont tous θ-conjugués alors

$$\mathcal{R}_{k,n}^\theta(\underline{\alpha}) \sim \mathcal{O}_{k,n}^\theta(\underline{y})$$

où $\underline{y} = (y_1, \ldots, y_n)$ avec $\forall j \in \{1, \ldots, n\}, \alpha_j = \beta^{y_j} = \theta(y_j)\beta y_j^{-1}$ pour un $\beta \in F$.

Démonstration.

Soit $\beta \in F$ tel que $\forall j \in \{1, \ldots, n\}, \exists y_j \in F^*, \alpha_j = \beta^{y_j} = \theta(y_j)\beta y_j^{-1}$ alors

$$\forall i \in \{1, \ldots, k\}, N_{i-1}^\theta(\alpha_j) = N_{i-1}^\theta(\beta)\theta^{i-1}(y_j)y_j^{-1}$$

$$V_{k,n}^\theta(\underline{\alpha}) = diag(N_{i-1}^\theta(\beta)) \times W_{k,n}^\theta(\underline{y}) \times \mathbf{diag}(\mathbf{y_j^{-1}})$$

□

Proposition

Soit $\underline{\alpha} \in F^n$ tel que $\mathrm{rang}(V_n^\theta(\underline{\alpha})) = n$.
Si les α_i sont tous θ-conjugués alors

$$\mathcal{R}_{k,n}^\theta(\underline{\alpha}) \sim \mathcal{O}_{k,n}^\theta(\underline{y})$$

où $\underline{y} = (y_1, \ldots, y_n)$ avec $\forall j \in \{1, \ldots, n\}, \alpha_j = \beta^{y_j} = \theta(y_j)\beta y_j^{-1}$ pour un $\beta \in F$.

Démonstration.

Soit $\beta \in F$ tel que $\forall j \in \{1, \ldots, n\}, \exists y_j \in F^*, \alpha_j = \beta^{y_j} = \theta(y_j)\beta y_j^{-1}$ alors

$$\forall i \in \{1, \ldots, k\}, N_{i-1}^\theta(\alpha_j) = N_{i-1}^\theta(\beta)\theta^{i-1}(y_j){y_j}^{-1}$$

$$V_{k,n}^\theta(\underline{\alpha}) = diag(N_{i-1}^\theta(\beta)) \times W_{k,n}^\theta(\underline{y}) \times \mathbf{diag}(\mathbf{y_j^{-1}})$$

□

Exemple de θ-code d'évaluation de longueur 12 sur $\mathbb{F}_{3^6} = \mathbb{F}_3(a)$ avec $\theta : x \mapsto x^3$ et $a^6 + 2\,a^4 + a^2 + 2\,a + 2 = 0$

$$\underline{\alpha} = (\underbrace{1, a^2, a^4, a^6, a^8, a^{10}}_{\underline{\xi}=(\theta(y_i)y_i^{-1})}, \underbrace{a, a^3, a^5, a^7, a^9, a^{11}}_{\underline{\zeta}=(\theta(y_i)ay_i^{-1})}),\ \underline{y} = (1, a, a^2, a^3, a^4, a^5)$$

$$\mathrm{rang}(V_{12}^{\theta}(\underline{\alpha})) = \mathrm{rang}(V_6^{\theta}(\underline{\xi})) + \mathrm{rang}(V_6^{\theta}(\underline{\zeta})) = 2 \times \mathrm{rang}(W_6^{\theta}(\underline{y})) = 12$$

$\mathcal{R}_{k,12}^{\theta}(\underline{\alpha})$ code de matrice génératrice $V_{k,12}^{\theta}(\underline{\alpha}) = (V_{k,6}^{\theta}(\underline{\xi}) | V_{k,6}^{\theta}(\underline{\zeta}))$

Si $k \leq 6$, alors

$$\begin{array}{ccccc} \mathcal{R}_{k,12}^{\theta}(\underline{\alpha}) & \subset & \mathcal{R}_{k,6}^{\theta}(\underline{\xi}) & \times & \mathcal{R}_{k,6}^{\theta}(\underline{\zeta}) \\ & & \wr & & \wr \\ & & \mathcal{O}_{k,6}^{\theta}(\underline{y}) & & \mathcal{O}_{k,6}^{\theta}(\underline{y}) \end{array}$$

$F = \mathbb{F}_{q^n}$

$\theta : x \mapsto x^q$

Gabidulin

$$\mathcal{O}^{\theta}_{k,n}(\underline{y}) \quad \overset{\text{si } \underline{\alpha} \ \theta\text{-conj}}{\sim} \quad \mathcal{R}^{\theta}_{k,n}(\underline{\alpha})$$

$$\| \qquad\qquad\qquad \|$$

$$\mathcal{O}^{\theta,\delta}_{k,n}(\underline{y}) \qquad \mathcal{R}^{\theta,\delta}_{k,n}(\underline{\alpha} - \beta)$$

(θ, δ)-codes d'évaluation $=$ θ-codes d'évaluation

θ-codes et (θ, δ)-codes modules

dualité ?

$F = \mathbb{F}_{q^n}$

$\theta : x \mapsto x^q$

Gabidulin

Max Rank Dist

si $\underline{\alpha}$ θ-conj

$\mathcal{O}^{\theta}_{k,n}(\underline{y}) \sim \mathcal{R}^{\theta}_{k,n}(\underline{\alpha})$

$\| \qquad \|$

$\mathcal{O}^{\theta,\delta}_{k,n}(\underline{y}) \qquad \mathcal{R}^{\theta,\delta}_{k,n}(\underline{\alpha} - \beta)$

(θ, δ)-codes d'évaluation $=$ θ-codes d'évaluation

Métriques

$c \in F^n$, $C \subset F^n$ code linéaire $[n, k]$, $\theta \in Aut(F)$.

Métrique de Hamming	Métrique rang (Gabidulin)
$\mathrm{w_H}(c) = \#\{i \in \{1, \ldots, n\}, c_i \neq 0\}$	$\mathrm{rang}^\theta(c) = \dim_{F^\theta}(c_1, \ldots, c_n)$
$\mathrm{w_H}(c) \leq n$	$\mathrm{rang}^\theta(c) \leq [F : F^\theta]$
$d_H = min_{c \in C, c \neq 0} \mathrm{w_H}(c)$ $\leq n - k + 1$	$d_r = min_{c \in C, c \neq 0} \mathrm{rang}^\theta(c)$ $\leq d_H$
MDS (Maximum Distance Separable) $d_H = n - k + 1$	MRD (Maximum Rank Distance) $d_r = n - k + 1$
C MDS $\Rightarrow$ $C^\perp$ MDS	C MRD $\Rightarrow$ $C^\perp$ MRD

Proposition

Soit $k \leq n \in \mathbb{N}^*$. Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in F^n$ tel que $\mathrm{rang}(V_n^\theta(\underline{\alpha})) = n$.
$\mathcal{R}_{k,n}^\theta(\underline{\alpha})$ est un code MDS : $d = n - k + 1$.

Démonstration.

- Soit $f = \mathrm{lclm}_{1 \leq i \leq k-1}(X - \alpha_i) \in F[X; \theta]$.
  Soit
  $$c = (\underbrace{f(\alpha_1)}_{0}, \ldots, \underbrace{f(\alpha_{k-1})}_{0}, f(\alpha_k), \ldots, f(\alpha_n)),$$
  alors $\mathrm{w_H}(c) = n - k + 1$.
  En effet, si $f(\alpha_k) = 0$, alors $\underbrace{\mathrm{lclm}_{1 \leq i \leq k}(X - \alpha_i)}_{\deg = k} \,|_d\, \underbrace{f}_{\deg = k-1} \rightarrow$ *impossible*
- On montre que le code ne possède pas de mot non nul de poids $< n - k + 1$.

□

Proposition

Soit $k \leq n \in \mathbb{N}^*$. Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in F^n$ tel que $\mathrm{rang}(V_n^\theta(\underline{\alpha})) = n$.
$\mathcal{R}_{k,n}^\theta(\underline{\alpha})$ est un code MDS : $d = n - k + 1$.

Démonstration.

- Soit $f = \mathrm{lclm}_{1 \leq i \leq k-1}(X - \alpha_i) \in F[X; \theta]$.
  Soit
  $$c = (\underbrace{f(\alpha_1)}_{0}, \ldots, \underbrace{f(\alpha_{k-1})}_{0}, f(\alpha_k), \ldots, f(\alpha_n)),$$
  alors $\mathrm{w_H}(c) = n - k + 1$.
  En effet, si $f(\alpha_k) = 0$, alors $\underbrace{\mathrm{lclm}_{1 \leq i \leq k}(X - \alpha_i)}_{\deg = k} \,|_d\, \underbrace{f}_{\deg = k-1} \rightarrow$ *impossible*
- On montre que le code ne possède pas de mot non nul de poids $< n - k + 1$.

□

Proposition

Soient $k \leq n \in \mathbb{N}^*$. Soit $\underline{y} = (y_1, \ldots, y_n) \in F^n$ tel que $\mathrm{rang}(W_n^\theta(\underline{y})) = n$.

1. (Gabidulin) Si $y_i = \theta^{i-1}(y)$ alors

$$\mathcal{O}_{k,n}^\theta(\underline{y})^\perp = (g)_n^\theta \quad \text{avec } g = \mathrm{lclm}_{1\leq i\leq k}(X - \theta(y_i)y_i^{-1}) \in F[X;\theta]$$

2. Si $y_i = \delta^{i-1}(y)$ alors

$$\mathcal{O}_{k,n}^\theta(\underline{y})^\perp = (g)_n^{\theta,\delta} \quad \text{avec } g = \mathrm{lclm}_{1\leq i\leq k}(X - \delta(y_i)y_i^{-1}) \in F[X;\theta,\delta]$$

Démonstration.

2. Soit $c \in F^n$, $\quad c \in \mathcal{O}_{k,n}^\theta(\underline{y})^\perp$

$$\begin{aligned}
&\Leftrightarrow \quad Wr_{k,n}^{\theta,\delta}(\underline{y}) \times c^T = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, \textstyle\sum_{j=1}^n \delta^{i-1}(y_j)c_j = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, \textstyle\sum_{j=1}^n \delta^{j-1}(y_i)c_j = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, \mathcal{L}_c(y_i) = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, c(\theta(y_i)y_i^{-1}) = 0\\
&\Leftrightarrow \quad c \in (g)_n^{\theta,\delta}
\end{aligned}$$

□

Proposition

Soient $k \leq n \in \mathbb{N}^*$. Soit $\underline{y} = (y_1, \ldots, y_n) \in F^n$ tel que $\mathrm{rang}(W_n^\theta(\underline{y})) = n$.

1. (Gabidulin) Si $y_i = \theta^{i-1}(y)$ alors

$$\mathcal{O}_{k,n}^\theta(\underline{y})^\perp = (g)_n^\theta \quad \text{avec } g = \mathrm{lclm}_{1\leq i\leq k}(X - \theta(y_i)y_i^{-1}) \in F[X;\theta]$$

2. Si $y_i = \delta^{i-1}(y)$ alors

$$\mathcal{O}_{k,n}^\theta(\underline{y})^\perp = (g)_n^{\theta,\delta} \quad \text{avec } g = \mathrm{lclm}_{1\leq i\leq k}(X - \delta(y_i)y_i^{-1}) \in F[X;\theta,\delta]$$

Démonstration.

2. Soit $c \in F^n$, $\quad c \in \mathcal{O}_{k,n}^\theta(\underline{y})^\perp$

$$\begin{aligned}
&\Leftrightarrow \quad Wr_{k,n}^{\theta,\delta}(\underline{y}) \times c^T = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, \textstyle\sum_{j=1}^n \delta^{\mathbf{i-1}}(\mathbf{y_j})c_j = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, \textstyle\sum_{j=1}^n \delta^{\mathbf{j-1}}(\mathbf{y_i})c_j = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, \mathcal{L}_c(y_i) = 0\\
&\Leftrightarrow \quad \forall i \in \{1,\ldots,k\}, c(\theta(y_i)y_i^{-1}) = 0\\
&\Leftrightarrow \quad c \in (g)_n^{\theta,\delta}
\end{aligned}$$

□

Proposition

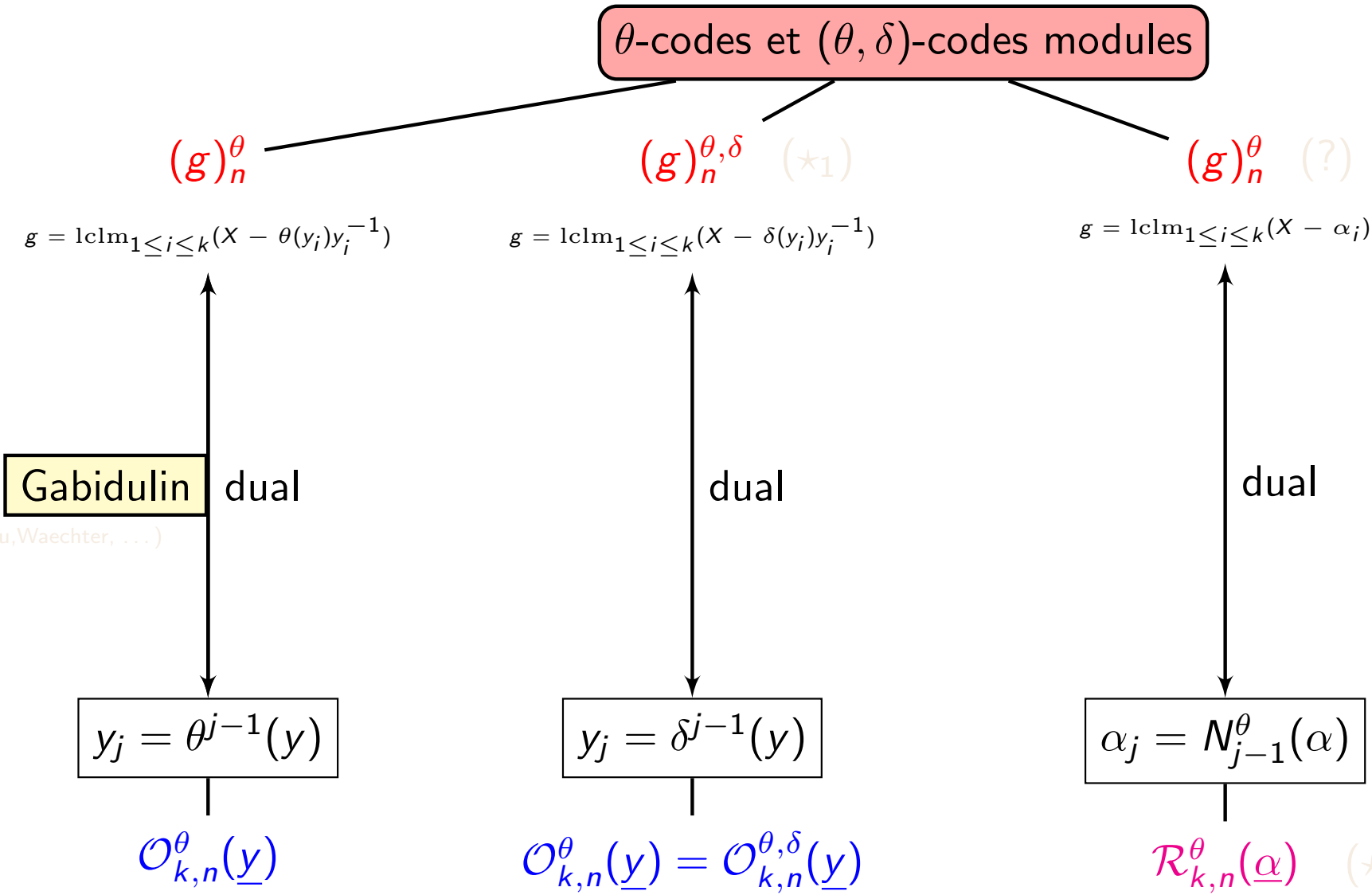
Soient $k \leq n \in \mathbb{N}^*$. Soit $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in F^n$ tel que $\mathrm{rang}(V_n^\theta(\underline{\alpha})) = n$
Si $\alpha_i = N_{i-1}^\theta(\alpha)$ alors

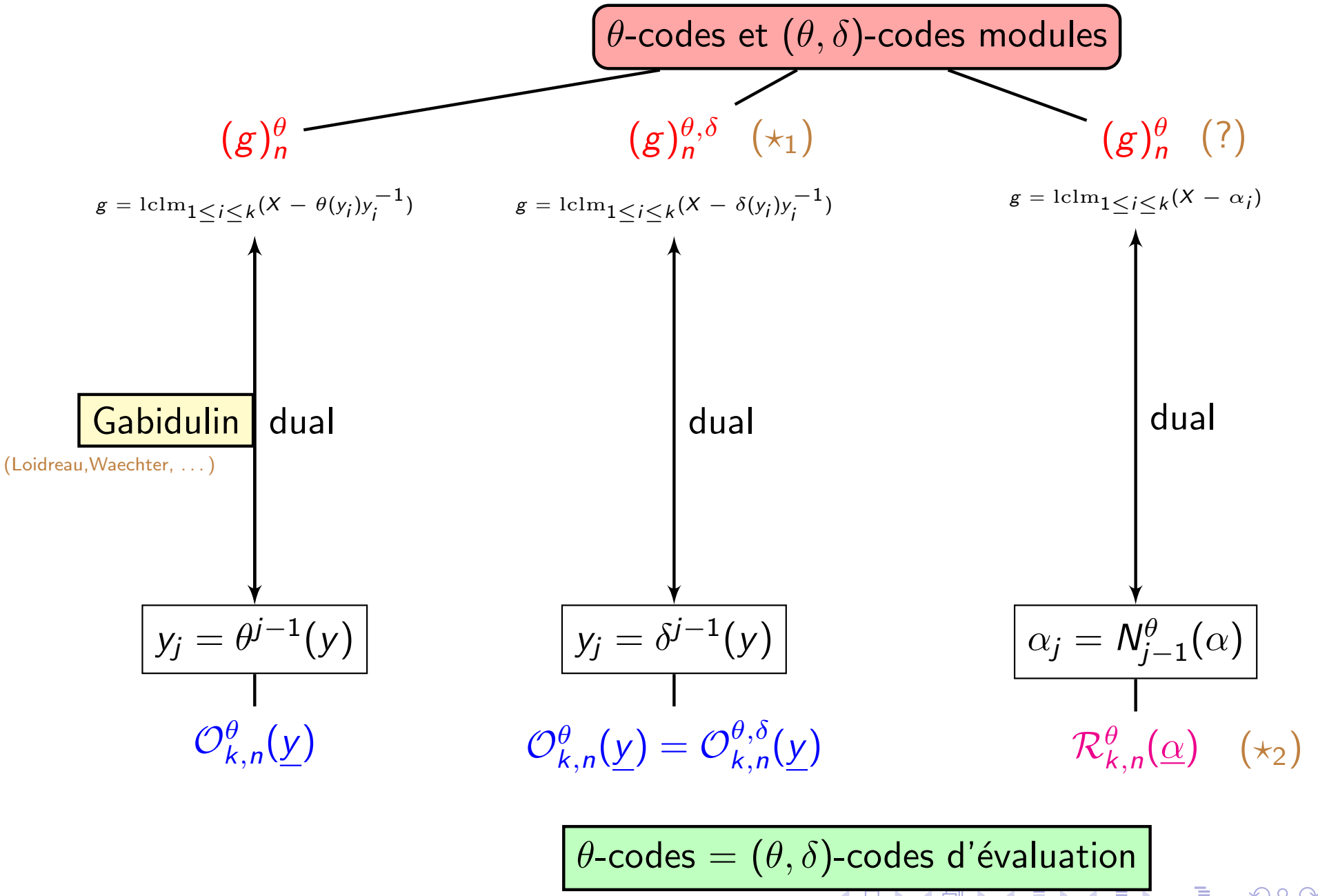
$$\mathcal{R}_{k,n}^\theta(\underline{\alpha})^\perp = (g)_n^\theta$$

avec $g = \mathrm{lclm}_{1 \leq i \leq k}(X - \alpha_i) \in F[X; \theta]$

Démonstration.

$V_{k,n}^\theta(\underline{\alpha}) = (N_{i-1}^\theta(\alpha_j))_{1 \leq i \leq k, 1 \leq j \leq n} = (N_{j-1}^\theta(\alpha_i))_{1 \leq i \leq k, 1 \leq j \leq n}$ □


θ-codes et (θ, δ)-codes modules
$(g)_n^{\theta}$
$(g)_n^{\theta,\delta}$ $(\star_1)$
$(g)_n^{\theta}$ (?)
$g = \mathrm{lclm}_{1\le i\le k}(X - \theta(y_i)y_i^{-1})$
$g = \mathrm{lclm}_{1\le i\le k}(X - \delta(y_i)y_i^{-1})$
$g = \mathrm{lclm}_{1\le i\le k}(X - \alpha_i)$
Gabidulin
dual
(Loidreau,Waechter, ...)
dual
dual
$y_j = \theta^{j-1}(y)$
$y_j = \delta^{j-1}(y)$
$\alpha_j = N_{j-1}^{\theta}(\alpha)$
$\mathcal{O}_{k,n}^{\theta}(\underline{y})$
$\mathcal{O}_{k,n}^{\theta}(\underline{y}) = \mathcal{O}_{k,n}^{\theta,\delta}(\underline{y})$
$\mathcal{R}_{k,n}^{\theta}(\underline{\alpha})$ $(\star_2)$
θ-codes = (θ, δ)-codes d'évaluation


θ-codes et (θ, δ)-codes modules
$(g)_n^\theta$
$(g)_n^{\theta,\delta}$ $(\star_1)$
$(g)_n^\theta$ (?)
$g = \mathrm{lclm}_{1\le i\le k}(X - \theta(y_i)y_i^{-1})$
$g = \mathrm{lclm}_{1\le i\le k}(X - \delta(y_i)y_i^{-1})$
$g = \mathrm{lclm}_{1\le i\le k}(X - \alpha_i)$
Gabidulin
(Loidreau,Waechter, . . .)
dual
dual
dual
$y_j = \theta^{j-1}(y)$
$y_j = \delta^{j-1}(y)$
$\alpha_j = N_{j-1}^\theta(\alpha)$
$\mathcal{O}_{k,n}^\theta(\underline{y})$
$\mathcal{O}_{k,n}^\theta(\underline{y}) = \mathcal{O}_{k,n}^{\theta,\delta}(\underline{y})$
$\mathcal{R}_{k,n}^\theta(\underline{\alpha})$ $(\star_2)$
θ-codes = (θ, δ)-codes d'évaluation

On considère $\mathcal{R}^{\theta}_{k,n}(\underline{\alpha})$ avec $\mathrm{rang}(V^{\theta}_{n}(\underline{\alpha})) = n \rightarrow$ code MDS

Pour simplifier, on suppose que tous les α_i sont non nuls.

Algorithme ($\star_2$)

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

Sortie : f

1 : Trouver $(q_0, \ldots q_n)$ solution du système linéaire à n équations :

$$\forall i \in \{1, \ldots, n\}, \sum_{j=0}^{k+t} q_j \, N_j^{\theta}(\alpha_i) + \sum_{j=0}^{t} q_{k+t+j+1} \, N_j^{\theta}\left(\theta(v_i)\alpha_i {v_i}^{-1}\right) v_i = 0$$

2 : $Q_0(X) \leftarrow \sum_{j=0}^{k+t} q_j X^j$

3 : $Q_1(X) \leftarrow \sum_{j=0}^{t} q_{j+1+k+t} X^j$

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

5 : **rendre** f

On considère $\mathcal{R}^{\theta}_{k,n}(\underline{\alpha})$ avec $\mathrm{rang}(V^{\theta}_{n}(\underline{\alpha})) = n \rightarrow$ code MDS

Pour simplifier, on suppose que tous les α_i sont non nuls.

Algorithme ($\star_2$)

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

Sortie : f

1 : Trouver $(q_0, \ldots q_n)$ solution du système linéaire à n équations :

$$\forall i \in \{1, \ldots, n\}, \sum_{j=0}^{k+t} q_j \, N_j^{\theta}(\alpha_i) + \sum_{j=0}^{t} q_{k+t+j+1} \, N_j^{\theta}\left(\theta(v_i)\alpha_i {v_i}^{-1}\right) v_i = 0$$

2 : $Q_0(X) \leftarrow \sum_{j=0}^{k+t} q_j X^j$

3 : $Q_1(X) \leftarrow \sum_{j=0}^{t} q_{j+1+k+t} X^j$

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

5 : **rendre** f

Preuve

$\rightarrow$ ce que l'on connaît : $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n), v = (v_1, \ldots, v_n) \in F^n$ tels que $\exists! f \in F[X;\theta]$ avec $\deg(f) < k$ et $\#\underbrace{\{i \in \{1, \ldots, n\}, v_i = f(\alpha_i)\}}_{I} > n - t - 1$

$\rightarrow$ ce que l'on cherche : f

- Soient $Q_0(X) = \sum_{j=0}^{k+t} q_j X^j$ et $Q_1(X) = \sum_{j=0}^{t} q_{j+1+k+t} X^j \in F[X;\theta]$ tels que

$$(*) \quad \forall i \in \{1, \ldots, n\}, \sum_{j=0}^{k+t} q_j \, N_j^{\theta}(\alpha_i) + \sum_{j=0}^{t} q_{k+t+j+1} \, N_j^{\theta}\left(\theta(v_i)\alpha_i {v_i}^{-1}\right) \, v_i = 0$$

$\rightarrow$ n équations linéaires en $k + t + 1 + t + 1 = n + 1$ inconnues

- Soit $R(X) = Q_0(X) + Q_1(X) \cdot f(X)$ (f inconnu, Q_0, Q_1 connus)

$\rightarrow \deg(R) \leq k + t = n - t - 1$

Preuve

$\rightarrow$ ce que l'on connaît : $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n), v = (v_1, \ldots, v_n) \in F^n$ tels que $\exists! f \in F[X;\theta]$ avec $\deg(f) < k$ et $\#\underbrace{\{i \in \{1, \ldots, n\}, v_i = f(\alpha_i)\}}_{I} > n - t - 1$

$\rightarrow$ ce que l'on cherche : f

- Soient $Q_0(X) = \sum_{j=0}^{k+t} q_j X^j$ et $Q_1(X) = \sum_{j=0}^{t} q_{j+1+k+t} X^j \in F[X;\theta]$ tels que

$$(*)\ \ \forall i \in \{1, \ldots, n\}, \sum_{j=0}^{k+t} q_j\, N_j^{\theta}(\alpha_i) + \sum_{j=0}^{t} q_{k+t+j+1}\, N_j^{\theta}\left(\theta(v_i)\alpha_i {v_i}^{-1}\right)\ v_i = 0$$

$\rightarrow$ n équations linéaires en $k + t + 1 + t + 1 = n + 1$ inconnues

- Soit $R(X) = Q_0(X) + Q_1(X) \cdot f(X)$ (f inconnu, Q_0, Q_1 connus)

$$\rightarrow \deg(R) \leq k + t = n - t - 1$$

$\longrightarrow$ ce que l'on cherche à montrer : $R = 0 \in F[X;\theta]$

$$\begin{aligned}
\forall i \in I, R(\alpha_i) &= Q_0(\alpha_i) + (Q_1 \cdot f)(\alpha_i) \\
&= Q_0(\alpha_i) + Q_1(\alpha_i^{f(\alpha_i)}) f(\alpha_i) && \text{(formule du produit de Lam)} \\
&= Q_0(\alpha_i) + Q_1(\theta(v_i)\alpha_i v_i^{-1}) v_i && \text{(car } v_i = f(\alpha_i) \text{ pour } i \in I) \\
&= 0 && \text{(d'après les équations}(*))
\end{aligned}$$

$\Rightarrow S := \mathrm{lclm}_{i \in I}(X - \alpha_i)$ divise R à droite

$\Rightarrow \deg(S) \leq \deg(R)$ ou $R = 0$.

De plus

$\deg(S) = \#I$ (car $\mathrm{rang}(V_n^\theta(\underline{\alpha})) = n$)

$\#I > deg(R)$,

donc $R = 0$.

- Conclusion :
  - construction de (θ, δ)-codes d'évaluation ;
  - construction de sous-familles de (θ, δ)-codes modules ;
  - des algorithmes de décodage $(\star_{1,2})$.

- Questions/perspectives :
  - Qu'apportent les θ-codes d'évaluation $\mathcal{R}^{\theta}_{k,n}(\underline{\alpha})$?
    $\longrightarrow$ sur $\mathbb{F}_{p^m}$ avec $\theta : x \mapsto x^p$, on a $n \leq (p-1)m + 1$ au lieu de
    - $n \leq p^m - 1$ pour les codes d'évaluation classiques ;
    - $n \leq m$ pour les codes de Gabidulin.

  - Qu'apporte l'algorithme $(\star_1)$?
    $\longrightarrow$ il existe des algorithmes de décodage pour les $O^{\theta}_{k,n}(\underline{y})^{\perp}$ en métrique rang !

  - Un algorithme de décodage $(?)$ serait-il intéressant ?

Merci pour votre attention !