About codes defined over skew polynomials.

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

Noncommutative rings and their applications
Lens 14th June - 16th June 2011

Plan.

Skew polynomials and linearized polynomials.

Gabidulin codes.
- Rank metric.
- Gabidulin codes (of linearized evaluation).
- Gabidulin q-cyclic codes.

Module θ-codes.
- Definition.
- θ-constacyclic and shortened θ-constacyclic codes.
- Dual code.
- Self-dual codes.

Skew polynomials.

- $\mathbb{F}_{q^m}$, finite field
- $\theta : a \mapsto a^q$, automorphism of $\mathbb{F}_{q^m}$
- $R = \mathbb{F}_{q^m}[X;\theta]$ Ore ring (1933)
  Addition : like in $\mathbb{F}_{q^m}[X]$
  Multiplication : $X \cdot a = \theta(a)\, X,\ a \in \mathbb{F}_{q^m}$
- Example
  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$

$$(X+\alpha)\cdot(X+\alpha^2) \quad = \quad X^2 + X\cdot\alpha^2 + \alpha\, X + \alpha^3$$

Skew polynomials.

- $\mathbb{F}_{q^m}$, finite field
- $\theta : a \mapsto a^q$, automorphism of $\mathbb{F}_{q^m}$
- $R = \mathbb{F}_{q^m}[X;\theta]$ Ore ring (1933)

  Addition : like in $\mathbb{F}_{q^m}[X]$

  Multiplication : $X \cdot a = \theta(a)\, X,\, a \in \mathbb{F}_{q^m}$
- Example

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

  $$(X+\alpha)\cdot(X+\alpha^2) \quad = \quad X^2 + X\cdot\alpha^2 + \alpha\, X + \alpha^3$$

Skew polynomials.

- $\mathbb{F}_{q^m}$, finite field
- $\theta : a \mapsto a^q$, automorphism of $\mathbb{F}_{q^m}$
- $R = \mathbb{F}_{q^m}[X;\theta]$ Ore ring (1933)
  Addition : like in $\mathbb{F}_{q^m}[X]$
  Multiplication : $X \cdot a = \theta(a)\, X, a \in \mathbb{F}_{q^m}$
- Example
  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$

$$(X+\alpha)\cdot(X+\alpha^2) \quad = \quad X^2 + X\cdot\alpha^2 + \alpha\, X + \alpha^3$$

Skew polynomials.

- $\mathbb{F}_{q^m}$, finite field
- $\theta : a \mapsto a^q$, automorphism of $\mathbb{F}_{q^m}$
- $R = \mathbb{F}_{q^m}[X;\theta]$ Ore ring (1933)
  Addition : like in $\mathbb{F}_{q^m}[X]$
  Multiplication : $X \cdot a = \theta(a)\, X, a \in \mathbb{F}_{q^m}$
- Example
  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$

$$(X+\alpha)\cdot(X+\alpha^2) \quad = \quad X^2 + X\cdot\alpha^2 + \alpha\, X + \alpha^3$$

Skew polynomials.

- $\mathbb{F}_{q^m}$, finite field
- $\theta : a \mapsto a^q$, automorphism of $\mathbb{F}_{q^m}$
- $R = \mathbb{F}_{q^m}[X; \theta]$ Ore ring (1933)
  Addition : like in $\mathbb{F}_{q^m}[X]$
  Multiplication : $X \cdot a = \theta(a)\, X, a \in \mathbb{F}_{q^m}$
- Example
  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X; \theta]$

$$(X + \alpha) \cdot (X + \alpha^2) \quad = \quad X^2 + \alpha^4\, X + \alpha\, X + \alpha^3$$

Skew polynomials.

- $\mathbb{F}_{q^m}$, finite field

- $\theta : a \mapsto a^q$, automorphism of $\mathbb{F}_{q^m}$

- $R = \mathbb{F}_{q^m}[X;\theta]$ Ore ring (1933)
  Addition : like in $\mathbb{F}_{q^m}[X]$
  Multiplication : $X \cdot a = \theta(a)\,X, a \in \mathbb{F}_{q^m}$

- Example
  $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$

$$
\begin{array}{rcl}
(X+\alpha)\cdot(X+\alpha^2) & = & X^2 + \alpha^4\,X + \alpha\,X + \alpha^3 \\
 & = & X^2 + 1
\end{array}
$$

Skew polynomials.

- Left Euclidean and right Euclidean divisions

  Notations : $g, f \in R$

  $g|_r f \Leftrightarrow \exists h \in R, f = h \cdot g$

  $g|_l f \Leftrightarrow \exists h \in R, f = g \cdot h$

- Factorisation in product of irreducible skew polynomials not unique

- Example

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

$$\begin{aligned} X^2+1 &= (X+\alpha)\cdot(X+\alpha^2) \\ &= (X+\alpha^2)\cdot(X+\alpha) \\ &= (X+1)\cdot(X+1) \end{aligned}$$

Skew polynomials.

- Left Euclidean and right Euclidean divisions

  Notations : $g, f \in R$

  $g|_r f \Leftrightarrow \exists h \in R, f = h \cdot g$

  $g|_l f \Leftrightarrow \exists h \in R, f = g \cdot h$

- Factorisation in product of irreducible skew polynomials not unique

- Example

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

$$\begin{aligned} X^2+1 &= (X+\alpha)\cdot(X+\alpha^2) \\ &= (X+\alpha^2)\cdot(X+\alpha) \\ &= (X+1)\cdot(X+1) \end{aligned}$$

Skew polynomials.

- Left Euclidean and right Euclidean divisions

  Notations : $g, f \in R$

  $g|_r f \Leftrightarrow \exists h \in R, f = h \cdot g$

  $g|_l f \Leftrightarrow \exists h \in R, f = g \cdot h$

- Factorisation in product of irreducible skew polynomials not unique

- Example

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

$$\begin{aligned} X^2 + 1 &= (X + \alpha) \cdot (X + \alpha^2) \\ &= (X + \alpha^2) \cdot (X + \alpha) \\ &= (X + 1) \cdot (X + 1) \end{aligned}$$

Skew polynomials and linearized polynomials.

Skew polynomials		Linearized polynomials
$R = \mathbb{F}_{q^m}[X;\theta], \theta : a \mapsto a^q$		$L = \mathbb{F}_{q^m}[Y^q]$
$(R, +, \cdot)$	$\longrightarrow$	$(L, +, \circ)$
X	$\longmapsto$	Y^q
$f = \sum f_i X^i$	$\longmapsto$	$\sum f_i Y^{q^i}$
$X \cdot a = a^q X$	$\longleftrightarrow$	$Y^q \circ a = a^q Y^q$

"Linear" evaluation

$$\alpha \in \mathbb{F}_{q^m}, \mathcal{L}_f(\alpha) = \sum_i f_i \theta^i(\alpha) = \sum_i f_i \alpha^{q^i}$$

Skew polynomials and linearized polynomials.

Skew polynomials		Linearized polynomials
$R = \mathbb{F}_{q^m}[X;\theta], \theta : a \mapsto a^q$		$L = \mathbb{F}_{q^m}[Y^q]$
$(R, +, \cdot)$	$\longrightarrow$	$(L, +, \circ)$
X	$\mapsto$	Y^q
$f = \sum f_i X^i$	$\mapsto$	$\sum f_i Y^{q^i}$
$X \cdot a = a^q X$	$\leftrightarrow$	$Y^q \circ a = a^q Y^q$

"Linear" evaluation

$$\alpha \in \mathbb{F}_{q^m}, \mathcal{L}_f(\alpha) = \sum_i f_i \theta^i(\alpha) = \sum_i f_i \alpha^{q^i}$$

Skew polynomials and linearized polynomials.

Gabidulin codes.

- Rank metric.
- Gabidulin codes (of linearized evaluation).
- Gabidulin q-cyclic codes.

Module θ-codes.

- Definition.
- θ-constacyclic and shortened θ-constacyclic codes.
- Dual code.
- Self-dual codes.

Rank metric.

- Gabidulin, *Theory of Codes with Maximum Rank Distance* 1985
  Berger, Loidreau, Wachter, ...

- $y \in (\mathbb{F}_{q^m})^n$, $C \subset (\mathbb{F}_{q^m})^n$ $[n, k]$ linear code

Hamming metric	Rank metric
$\mathrm{w_H}(y)$ = nbe of nonzero coordinates of y	$\mathrm{rank(y\,;\,q)}$ = maximum nbe of $\mathbb{F}_q$ -linearly independent coordinates of y
$\mathrm{w_H}(y) \leq n$	$\mathrm{rang}(y; q) \leq m$
$d_H = min_{c\in C, c\neq 0}\mathrm{w_H}(c) \leq n-k+1$	$d_r = min_{c\in C, c\neq 0}\mathrm{rank}(c; q) \leq d_H$
MDS : $d_H = n-k+1$	MRD : $d_r = n-k+1$

Rank metric.

- Gabidulin, *Theory of Codes with Maximum Rank Distance* 1985
  Berger, Loidreau, Wachter, ...

- $y \in (\mathbb{F}_{q^m})^n$, $C \subset (\mathbb{F}_{q^m})^n$ $[n, k]$ linear code

Hamming metric	Rank metric
$\mathrm{w_H}(y)$ = nbe of nonzero coordinates of y	$\mathrm{rank}(\mathrm{y}\,;\,\mathrm{q})$ = maximum nbe of $\mathbb{F}_q$ -linearly independent coordinates of y
$\mathrm{w_H}(y) \leq n$	$\mathrm{rang}(y; q) \leq m$
$d_H = min_{c \in C, c \neq 0} \mathrm{w_H}(c) \leq n - k + 1$	$d_r = min_{c \in C, c \neq 0} \mathrm{rank}(c; q) \leq d_H$
MDS : $d_H = n - k + 1$	MRD : $d_r = n - k + 1$

Skew polynomials and linearized polynomials.

Gabidulin codes.

- Rank metric.
- Gabidulin codes (of linearized evaluation).
- Gabidulin q-cyclic codes.

Module θ-codes.

- Definition.
- θ-constacyclic and shortened θ-constacyclic codes.
- Dual code.
- Self-dual codes.

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \ldots, 0, \mathcal{L}_f(y_k), \ldots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n - k + 1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \ldots, 0, \mathcal{L}_f(y_k), \ldots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \dots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \ldots, 0, \mathcal{L}_f(y_k), \ldots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $\quad (\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $(\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \ldots, 0, \mathcal{L}_f(y_k), \ldots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \dots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $(\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \dots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \dots, 0, \mathcal{L}_f(y_k), \dots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$ $(\mathrm{rang}(y;q) = n)$
  $n \leq m$
- $1 \leq k \leq n$
- $\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$
  Gabidulin code (of linearized evaluation)
- Let $f \in R$, $\deg(f) = k-1$ such that $\mathcal{L}_f(y_1) = \cdots = \mathcal{L}_f(y_{k-1}) = 0$
  $c = (0, \ldots, 0, \mathcal{L}_f(y_k), \ldots, \mathcal{L}_f(y_n)) \in \mathcal{G}_{n,k}$
  $$\sum_{i=k}^{n} \lambda_i \mathcal{L}_f(y_i) = 0, \lambda_i \in \mathbb{F}_q \Rightarrow \mathcal{L}_f\left(\sum_{i=k}^{n} \lambda_i y_i\right) = 0, \lambda_i \in \mathbb{F}_q \quad \Rightarrow \lambda_i = 0$$
  $\mathrm{rank}(c;q) = n-k+1$

Gabidulin code (of linearized evaluation).

$y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$

$\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$

- $\mathcal{G}_{n,k}$ is a MRD (Maximum Rank Distance) code.
- The dual of a Gabidulin code (of linearized evaluation) is a Gabidulin code (of linearized evaluation).
- If $n = m$, if $y_i = \theta^{i-1}(y)$ normal basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$, then the dual of $\mathcal{G}_{n,k}$ is a q-cyclic code.

Gabidulin code (of linearized evaluation).

$y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$

$\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$

- $\mathcal{G}_{n,k}$ is a MRD (Maximum Rank Distance) code.
- The dual of a Gabidulin code (of linearized evaluation) is a Gabidulin code (of linearized evaluation).
- If $n = m$, if $y_i = \theta^{i-1}(y)$ normal basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$, then the dual of $\mathcal{G}_{n,k}$ is a q-cyclic code.

Gabidulin code (of linearized evaluation).

$y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$

$\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$

- $\mathcal{G}_{n,k}$ is a MRD (Maximum Rank Distance) code.
- The dual of a Gabidulin code (of linearized evaluation) is a Gabidulin code (of linearized evaluation).
- If $n = m$, if $y_i = \theta^{i-1}(y)$ normal basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$, then the dual of $\mathcal{G}_{n,k}$ is a q-cyclic code.

Gabidulin code (of linearized evaluation).

$y_1, \ldots, y_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$

$\mathcal{G}_{n,k} = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in R, \deg(f) \leq k-1\}$

- $\mathcal{G}_{n,k}$ is a MRD (Maximum Rank Distance) code.
- The dual of a Gabidulin code (of linearized evaluation) is a Gabidulin code (of linearized evaluation).
- If $n = m$, if $y_i = \theta^{i-1}(y)$ normal basis of $\mathbb{F}_{q^n}/\mathbb{F}_q$, then the dual of $\mathcal{G}_{n,k}$ is a q-cyclic code.

Gabidulin linear q-cyclic code.

- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$
- C linear q-cyclic

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

Gabidulin linear q-cyclic code.

- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$
- C linear q-cyclic

$$(c_0, \ldots, c_{n-1}) \quad \in \quad C \quad \Rightarrow \quad (c_{n-1}^q, c_0^q, \ldots, c_{n-2}^q) \in C$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$\begin{array}{ccccc} (c_0, \ldots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \ldots, c_{n-2}^q) \in C \\ \updownarrow & & & & \\ c_0 + \cdots + c_{n-1}X^{n-1} & & & & \end{array}$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$
\begin{array}{ccccc}
(c_0, \dots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \dots, c_{n-2}^q) \in C \\
\updownarrow & & \updownarrow & & \\
c_0 + \cdots + c_{n-1}X^{n-1} & \in & C(X) & & \\
 & & \bigcap & & \\
 & & R/(X^n - 1) & & \\
 & & \text{quotient ring} & &
\end{array}
$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$
\begin{array}{ccccc}
(c_0, \ldots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \ldots, c_{n-2}^q) \in C \\
\updownarrow & & \updownarrow & & \\
c_0 + \cdots + c_{n-1}X^{n-1} & \in & C(X) & & \\
 & & \bigcap & & \\
 & & R/(X^n - 1) & & \\
 & & \text{quotient ring} & & \\
 & & (X^n \cdot a = \theta^n(a)\, X^n) & &
\end{array}
$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$\begin{array}{ccccc}
(c_0, \dots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \dots, c_{n-2}^q) \in C \\
\updownarrow & & \updownarrow & & \\
c_0 + \dots + c_{n-1}X^{n-1} & \in & C(X) & & \\
 & & \bigcap & & \\
 & & R/(X^n - 1) & & \\
 & & \text{quotient ring} & & \\
 & & (X^n \cdot a = a\, X^n) & &
\end{array}$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$
\begin{array}{ccccc}
(c_0, \ldots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \ldots, c_{n-2}^q) \in C \\
\updownarrow & & \updownarrow & & \updownarrow \\
c_0 + \cdots + c_{n-1}X^{n-1} & \in & C(X) & \Rightarrow & c_{n-1}^q + c_0^q X + \cdots + c_{n-2}^q X^{n-1} \\
 & & \bigcap & & \| \\
 & & R/(X^n - 1) & & X \cdot (c_0 + \cdots + c_{n-1}X^{n-1}) \in C(X)
\end{array}
$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$\begin{array}{ccccc}
(c_0, \dots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \dots, c_{n-2}^q) \in C \\
\updownarrow & & \updownarrow & & \updownarrow \\
c_0 + \cdots + c_{n-1}X^{n-1} & \in & C(X) & \Rightarrow & c_{n-1}^q + c_0^q X + \cdots + c_{n-2}^q X^{n-1} \\
 & & \bigcap & & \| \\
 & & R/(X^n - 1) & & X \cdot (c_0 + \cdots + c_{n-1}X^{n-1}) \in C(X)
\end{array}$$

Gabidulin q-cyclic linear code.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $C \subset (\mathbb{F}_{q^m})^n$ linear, $n = m$

$$
\begin{array}{ccccc}
(c_0, \dots, c_{n-1}) & \in & C & \Rightarrow & (c_{n-1}^q, c_0^q, \dots, c_{n-2}^q) \in C \\
\updownarrow & & \updownarrow & & \updownarrow \\
c_0 + \cdots + c_{n-1}X^{n-1} & \in & C(X) & \Rightarrow & c_{n-1}^q + c_0^q X + \cdots + c_{n-2}^q X^{n-1} \\
 & & \bigcap & & \| \\
 & & R/(X^n - 1) & & X \cdot (c_0 + \cdots + c_{n-1}X^{n-1}) \in C(X)
\end{array}
$$

- $C(X)$ left principal ideal of the quotient ring $R/(X^n - 1)$
- $C(X) = (g)/(X^n - 1)$, $g|_r X^n - 1$, generator polynomial

Gabidulin q-cyclic code.

- A generator matrix of a $[n = m, k]$ q-cyclic linear code of Gabidulin over $\mathbb{F}_{q^m}$ with generator polynomial $g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}$ is

$$\begin{pmatrix} g_0 & \dots & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0^q & \dots & \dots & g_{n-k}^q & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & g_0^{q^{k-1}} & \dots & \dots & g_{n-k}^{q^{k-1}} \end{pmatrix}$$

- The dual of a q-cyclic linear code $[n = m, k]$ generated by g is a q-cyclic linear code generated by h^* where

$$h \cdot g = g \cdot h = X^n - 1$$
$$h^* = \sum X^{k-i} \cdot h_i$$

Gabidulin q-cyclic code.

- A generator matrix of a $[n = m, k]$ q-cyclic linear code of Gabidulin over $\mathbb{F}_{q^m}$ with generator polynomial $g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}$ is

$$\begin{pmatrix} g_0 & \dots & \dots & g_{n-k} & 0 & \dots & 0 \\ 0 & g_0^q & \dots & \dots & g_{n-k}^q & \ddots & \vdots \\ \vdots & \ddots & \ddots & & & \ddots & 0 \\ 0 & \dots & 0 & g_0^{q^{k-1}} & \dots & \dots & g_{n-k}^{q^{k-1}} \end{pmatrix}$$

- The dual of a q-cyclic linear code $[n = m, k]$ generated by g is a q-cyclic linear code generated by h^* where

$$h \cdot g = g \cdot h = X^n - 1$$
$$h^* = \sum X^{k-i} \cdot h_i$$

Module θ-codes.

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

- A conjecture given in *Codes as modules over skew polynomial rings*, Proceedings of the 12th IMA conference on Cryptography and Coding, Cirencester, 2009, LNCS ; B., Ulmer :

  "We conjecture than an Euclidean self-dual module θ-code is a module θ-constacyclic code."

$\rightarrow$ Aim today :

- definition of module θ-codes
- definition of θ-constacyclic and shortened θ-constacyclic codes
- proof of the conjecture
- construction of self-dual module θ-codes

Module θ-codes.

- 2007 - : Ulmer, Solé, Loidreau, Geiselmann, Chaussade, B., ...
- A conjecture given in *Codes as modules over skew polynomial rings*, Proceedings of the 12th IMA conference on Cryptography and Coding, Cirencester, 2009, LNCS ; B., Ulmer :

  "We conjecture than an Euclidean self-dual module θ-code is a module θ-constacyclic code."

→ Aim today :

- definition of module θ-codes
- definition of θ-constacyclic and shortened θ-constacyclic codes
- proof of the conjecture
- construction of self-dual module θ-codes

Module θ-codes.

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

- A conjecture given in *Codes as modules over skew polynomial rings*, Proceedings of the 12th IMA conference on Cryptography and Coding, Cirencester, 2009, LNCS ; B., Ulmer :

  "We conjecture than an Euclidean self-dual module θ-code is a module θ-constacyclic code."

$\longrightarrow$ Aim today :

- definition of module θ-codes
- definition of θ-constacyclic and shortened θ-constacyclic codes
- proof of the conjecture
- construction of self-dual module θ-codes

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $g \in R$, $g_0 \neq 0$, $g|_r X^n - 1$

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $g \in R$, $g_0 \neq 0$, $g|_r X^n - 1$

$n = m$	$R/(X^n - 1)$	quotient ring
	$C(X) = (g)/(X^n - 1)$	left principal ideal
	C	q-cyclic code

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $g \in R$, $g_0 \neq 0$, $g|_r X^n - 1$

any n	$R/R(X^n - 1)$	left R-module
	$C(X) = Rg/R(X^n - 1)$	left R-submodule
	C	θ-cyclic code

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $g \in R$, $g_0 \neq 0$, $g|_r X^n - a, a \in \mathbb{F}^*_{q^m}$

any n	$R/R(X^n - a)$	left R-module
	$C(X) = Rg/R(X^n - a)$	left R-submodule
	C	θ-constacyclic code

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $g \in R$, $g_0 \neq 0$, $g|_r f, \deg(f) = n$

any n	R/Rf	left R-module
	$C(X) = Rg/Rf$	left R-submodule
	C	module θ-code

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $f \in R$, $\deg(f) = n$.
  $g \in R$, $g_0 \neq 0$, $g|_r f$
  $k = n - \deg(g)$
- $C(X) = Rg/Rf$, left R-submodule of R/Rf
- $C(X) = \{m \cdot g / \deg(m) \leq k-1\}$
  $C = \left\{ c \in (\mathbb{F}_{q^m})^n, \sum_{i=0}^{n-1} c_i X^i \in C(X) \right\}$ module θ-code
- Notation

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

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $f \in R$, $\deg(f) = n$.
  $g \in R$, $g_0 \neq 0$, $g|_r f$
  $k = n - \deg(g)$
- $C(X) = Rg/Rf$, left R-submodule of R/Rf
- $C(X) = \{m \cdot g / \deg(m) \leq k-1\}$
  $C = \left\{ c \in (\mathbb{F}_{q^m})^n, \sum_{i=0}^{n-1} c_i X^i \in C(X) \right\}$ module θ-code
- Notation

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

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $f \in R$, $\deg(f) = n$.
  $g \in R$, $g_0 \neq 0$, $g|_r f$
  $k = n - \deg(g)$
- $C(X) = Rg/Rf$, left R-submodule of R/Rf
- $C(X) = \{m \cdot g / \deg(m) \leq k-1\}$
  $C = \left\{ c \in (\mathbb{F}_{q^m})^n, \sum_{i=0}^{n-1} c_i X^i \in C(X) \right\}$ module θ-code
- Notation

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

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $f \in R$, $\deg(f) = n$.
  $g \in R$, $g_0 \neq 0$, $g|_r f$
  $k = n - \deg(g)$
- $C(X) = Rg/Rf$, left R-submodule of R/Rf
- $C(X) = \{m \cdot g / \deg(m) \leq k-1\}$

  $$C = \left\{ c \in (\mathbb{F}_{q^m})^n, \sum_{i=0}^{n-1} c_i X^i \in C(X) \right\}$$ module θ-code
- Notation

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

Module θ-codes.

- $R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$
- $f \in R$, $\deg(f) = n$.
  $g \in R$, $g_0 \neq 0$, $g|_r f$
  $k = n - \deg(g)$
- $C(X) = Rg/Rf$, left R-submodule of R/Rf
- $C(X) = \{m \cdot g / \deg(m) \leq k-1\}$
  $C = \left\{ c \in (\mathbb{F}_{q^m})^n, \sum_{i=0}^{n-1} c_i X^i \in C(X) \right\}$ module θ-code
- Notation

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

Generator matrix.

$$C = (g)_{n,\theta},\ k = n - \deg(g)$$

Generator matrix.

$C = (g)_{n,\theta}$, $k = n - \deg(g)$

$$
\begin{aligned}
&g = g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}\\
&X \cdot g = \theta(g_0) X + \theta(g_1) X^2 + \cdots + \theta(g_{n-k}) X^{n-k+1}\\
&\vdots\\
&X^{k-1} \cdot g = \theta^{k-1}(g_0) X^{k-1} + \theta^{k-1}(g_1) X^k + \cdots + \theta^{k-1}(g_{n-k}) X^{n-1}
\end{aligned}
$$

Generator matrix.

$$C = (g)_{n,\theta},\ k = n - \deg(g)$$

$$g = g_0 + g_1 X + \cdots + g_{n-k} X^{n-k}$$
$$X \cdot g = \theta(g_0) X + \theta(g_1) X^2 + \cdots + \theta(g_{n-k}) X^{n-k+1}$$
$$\vdots$$
$$X^{k-1} \cdot g = \theta^{k-1}(g_0) X^{k-1} + \theta^{k-1}(g_1) X^k + \cdots + \theta^{k-1}(g_{n-k}) X^{n-1}$$

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

Shortened codes and punctured codes.

C' $[n', k']$ linear code with generator matrix G' ; $n \leq n'$

shortened code	punctured code
$C = \rho_{n' \to n}(C')$	$C = \pi_{n' \to n}(C')$
$c \in C \Updownarrow (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in C'$	$c \in C \Updownarrow (c_0, \ldots, c_{n-1}, c_n, \ldots, c_{n'}) \in C'$
$[n, k]$, $n' - n = k' - k$	$[n, k = k']$
$G = G'\|_{[1..k],[1..n]}$	$G = G'\|_{[1..n]}$

θ-constacyclic codes.

- $\exists a \in \mathbb{F}_{q^m}^*, \; g|_r X^n - a$

- $(c_0, c_1, \cdots, c_{n-1}) \in (g)_{n,\theta}$
  $\Rightarrow (a\,\theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in (g)_{n,\theta}$

- $(g)_{n,\theta}$: θ-constacyclic code ; if $a = 1$, θ-cyclic code

- q-cyclic code of Gabidulin = θ-cyclic code with $n = m$

- Notation

$$(g)_{n,\theta,c}$$

θ-constacyclic codes.

- $\exists a \in \mathbb{F}_{q^m}^*,\ g|_r X^n - a$
- $(c_0, c_1, \cdots, c_{n-1}) \in (g)_{n,\theta}$
  $\Rightarrow (a\,\theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in (g)_{n,\theta}$
- $(g)_{n,\theta}$: θ-constacyclic code ; if $a = 1$, θ-cyclic code
- q-cyclic code of Gabidulin = θ-cyclic code with $n = m$
- Notation

$$(g)_{n,\theta,c}$$

θ-constacyclic codes.

- $\exists a \in \mathbb{F}_{q^m}^*$, $g|_r X^n - a$
- $(c_0, c_1, \cdots, c_{n-1}) \in (g)_{n,\theta}$
  $\Rightarrow (a\,\theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in (g)_{n,\theta}$
- $(g)_{n,\theta}$: θ-constacyclic code ; if $a = 1$, θ-cyclic code
- q-cyclic code of Gabidulin $=$ θ-cyclic code with $n = m$
- Notation

$$(g)_{n,\theta,c}$$

θ-constacyclic codes.

- $\exists a \in \mathbb{F}_{q^m}^*$, $g|_r X^n - a$
- $(c_0, c_1, \cdots, c_{n-1}) \in (g)_{n,\theta}$
  $\Rightarrow (a\,\theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in (g)_{n,\theta}$
- $(g)_{n,\theta}$: θ-constacyclic code ; if $a = 1$, θ-cyclic code
- q-cyclic code of Gabidulin = θ-cyclic code with $n = m$
- Notation

$$(g)_{n,\theta,c}$$

θ-constacyclic codes.

- $\exists a \in \mathbb{F}_{q^m}^*$, $g|_r X^n - a$

- $(c_0, c_1, \cdots, c_{n-1}) \in (g)_{n,\theta}$
  $\Rightarrow (a\, \theta(c_{n-1}), \theta(c_0), \theta(c_1), \ldots, \theta(c_{n-2})) \in (g)_{n,\theta}$

- $(g)_{n,\theta}$: θ-constacyclic code ; if $a = 1$, θ-cyclic code

- q-cyclic code of Gabidulin = θ-cyclic code with $n = m$

- Notation

$$(g)_{n,\theta,c}$$

Shortened θ-constacyclic codes.

- $\forall a \in \mathbb{F}_{q^m}^*$, $g \nmid_r X^n - a$

- $\exists n' > n, g|_r X^{n'} - 1$

$$g|_r \tilde{g},\ \tilde{g}_0 \neq 0, \tilde{g} \in \mathbb{F}_q[X^m]\ (\tilde{g},\ bound\ of\ g)$$
$$\tilde{g}|X^{n'} - 1 \in \mathbb{F}_q[X^m],\ n' > n$$
$$\tilde{g}|_r X^{n'} - 1\ because\ \theta(\tilde{g}_i) = \tilde{g}_i$$

- $(g)_{n,\theta}$, shortened θ-constacyclic code :

$(g)_{n,\theta} = \left\{c \in (\mathbb{F}_{q^m})^n, (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in (g)_{n',\theta,c}\right\}$

$$(g)_{n,\theta} = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$$

Shortened θ-constacyclic codes.

- $\forall a \in \mathbb{F}_{q^m}^*$, $g \not|_r X^n - a$

- $\exists n' > n, g|_r X^{n'} - 1$

  $g|_r \tilde{g}$, $\tilde{g}_0 \neq 0, \tilde{g} \in \mathbb{F}_q[X^m]$ ($\tilde{g}$, bound of g)
  $\tilde{g}|X^{n'} - 1 \in \mathbb{F}_q[X^m]$, $n' > n$
  $\tilde{g}|_r X^{n'} - 1$ because $\theta(\tilde{g}_i) = \tilde{g}_i$

- $(g)_{n,\theta}$, shortened θ-constacyclic code :
  $(g)_{n,\theta} = \left\{c \in (\mathbb{F}_{q^m})^n, (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in (g)_{n',\theta,c}\right\}$

$$(g)_{n,\theta} = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$$

Shortened θ-constacyclic codes.

- $\forall a \in \mathbb{F}_{q^m}^*$, $g \nmid_r X^n - a$

- $\exists n' > n, g|_r X^{n'} - 1$

$$g|_r \tilde{g},\ \tilde{g}_0 \neq 0, \tilde{g} \in \mathbb{F}_q[X^m] \ (\tilde{g},\ \textit{bound of } g)$$
$$\tilde{g}|X^{n'} - 1 \in \mathbb{F}_q[X^m],\ n' > n$$
$$\tilde{g}|_r X^{n'} - 1 \ \textit{because } \theta(\tilde{g}_i) = \tilde{g}_i$$

- $(g)_{n,\theta}$, shortened θ-constacyclic code :
$(g)_{n,\theta} = \left\{c \in (\mathbb{F}_{q^m})^n, (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in (g)_{n',\theta,c}\right\}$

$$(g)_{n,\theta} = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$$

Shortened θ-constacyclic codes.

- $\forall a \in \mathbb{F}_{q^m}^*$, $g \nmid_r X^n - a$

- $\exists n' > n, g|_r X^{n'} - 1$

$$g|_r \tilde{g},\ \tilde{g}_0 \neq 0, \tilde{g} \in \mathbb{F}_q[X^m]\ (\tilde{g},\ \textit{bound of } g)$$
$$\tilde{g}|X^{n'} - 1 \in \mathbb{F}_q[X^m],\ n' > n$$
$$\tilde{g}|_r X^{n'} - 1 \ \textit{because}\ \theta(\tilde{g}_i) = \tilde{g}_i$$

- $(g)_{n,\theta}$, shortened θ-constacyclic code :
$(g)_{n,\theta} = \left\{c \in (\mathbb{F}_{q^m})^n, (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in (g)_{n',\theta,c}\right\}$

$$(g)_{n,\theta} = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$$

Example.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $X^4 - 1 = (X^2 + \alpha^2 X + \alpha^2) \cdot \underbrace{(X^2 + \alpha^2 X + \alpha)}_{g}$
- $(g)_{4,\theta,c}$ $[4,2,3]_4$ θ-cyclic code

$$G_{g,4,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

- $(g)_{3,\theta}$ $[3,1,3]_4$ shortened θ-cyclic code

$$G_{g,3,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 \end{pmatrix}$$

Example.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $X^4 - 1 = (X^2 + \alpha^2 X + \alpha^2) \cdot \underbrace{(X^2 + \alpha^2 X + \alpha)}_{g}$
- $(g)_{4,\theta,c}$ $[4,2,3]_4$ θ-cyclic code

$$G_{g,4,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

- $(g)_{3,\theta}$ $[3,1,3]_4$ shortened θ-cyclic code

$$G_{g,3,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 \end{pmatrix}$$

Example.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $X^4 - 1 = (X^2 + \alpha^2 X + \alpha^2) \cdot \underbrace{(X^2 + \alpha^2 X + \alpha)}_{g}$
- $(g)_{4,\theta,c}$ $[4,2,3]_4$ θ-cyclic code

$$G_{g,4,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

- $(g)_{3,\theta}$ $[3,1,3]_4$ shortened θ-cyclic code

$$G_{g,3,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 \end{pmatrix}$$

Example.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $X^4 - 1 = (X^2 + \alpha^2 X + \alpha^2) \cdot \underbrace{(X^2 + \alpha^2 X + \alpha)}_{g}$
- $(g)_{4,\theta,c}$ $[4,2,3]_4$ θ-cyclic code

$$G_{g,4,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

- $(g)_{3,\theta}$ $[3,1,3]_4$ shortened θ-cyclic code

$$G_{g,3,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 \end{pmatrix}$$

Example.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $X^4 - 1 = (X^2 + \alpha^2 X + \alpha^2) \cdot \underbrace{(X^2 + \alpha^2 X + \alpha)}_{g}$
- $(g)_{4,\theta,c}$ $[4,2,3]_4$ θ-cyclic code

$$G_{g,4,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 & 0 \\ 0 & \alpha^2 & \alpha & 1 \end{pmatrix}$$

- $(g)_{3,\theta}$ $[3,1,3]_4$ shortened θ-cyclic code

$$G_{g,3,\theta} = \begin{pmatrix} \alpha & \alpha^2 & 1 \end{pmatrix}$$

$R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$

Module θ-code

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

$n = m$

q-cyclic — **θ-constacyclic** — **shortened θ-constacyclic**

$C = (g)_{n,\theta,c}$ | $C = (g)_{n,\theta,c}$ | $C = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$

dual (G.) | dual | dual

q-cyclic | $C^{\perp}$? | $C^{\perp}$?

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

$R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$

Module θ-code

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

$n = m$

q-cyclic

θ-constacyclic

shortened θ-constacyclic

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

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

$C = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$

dual (G.)

dual

dual

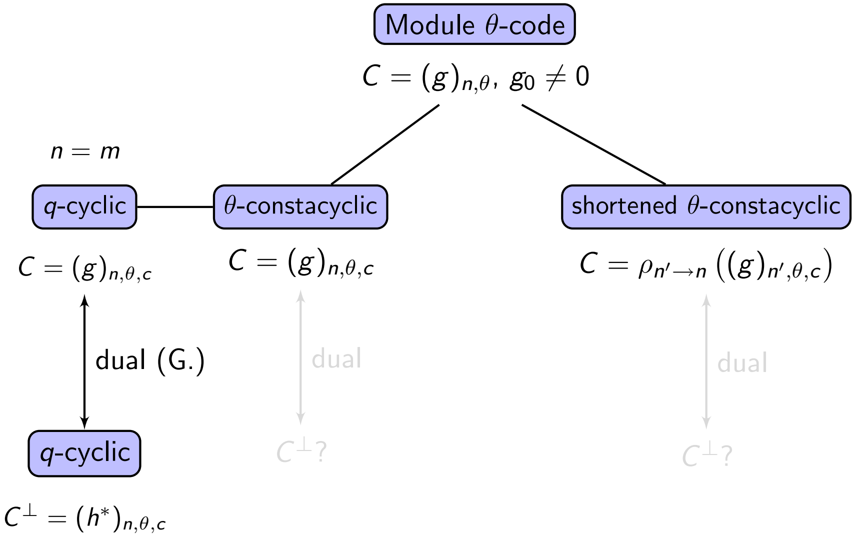
q-cyclic

$C^\perp?$

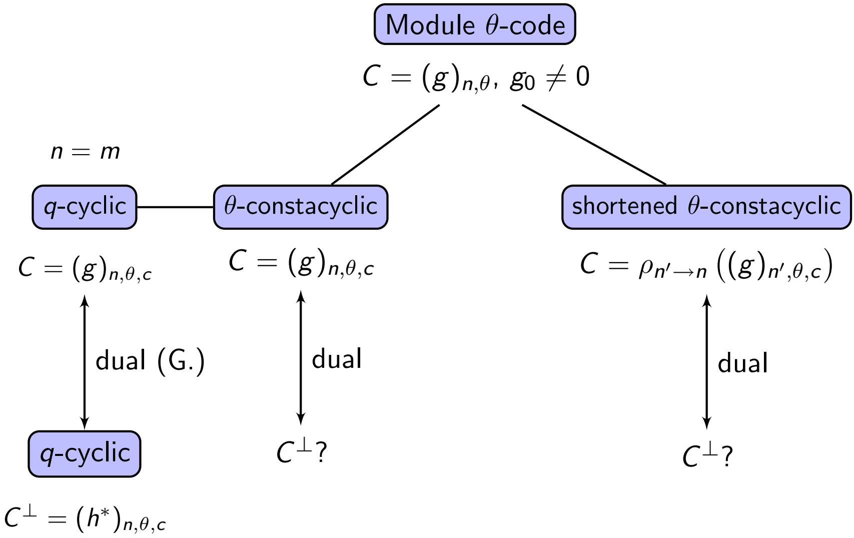
$C^\perp?$

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

$R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$



$R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$



Skew polynomials and linearized polynomials.

Gabidulin codes.

- Rank metric.
- Gabidulin codes (of linearized evaluation).
- Gabidulin q-cyclic codes.

Module θ-codes.

- Definition.
- θ-constacyclic and shortened θ-constacyclic codes.
- Dual code.
- Self-dual codes.

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}_{q^m}^*$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b, b \in \mathbb{F}_{q^m}^*$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R : h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}^*_{q^m}$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b,\ b \in \mathbb{F}^*_{q^m}$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R : h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}_{q^m}^*$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b, b \in \mathbb{F}_{q^m}^*$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R : h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}_{q^m}^*$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b, b \in \mathbb{F}_{q^m}^*$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R$: $h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}^*_{q^m}$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b, b \in \mathbb{F}^*_{q^m}$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R$: $h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}_{q^m}^*$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b, b \in \mathbb{F}_{q^m}^*$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R$: $h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a θ-constacyclic code is θ-constacyclic.

- Proof

  let $C = (g)_{n,\theta,c}$ *and let* $a \in \mathbb{F}_{q^m}^*$ *such that* $g|_r X^n - a$

  $g|_r X^n - a \Leftrightarrow g|_l X^n - b, b \in \mathbb{F}_{q^m}^*$

  Let $h \in R$ *be such that* $g \cdot h = X^n - b$, $\deg(h) = k$

  Let h^* *be the skew reciprocal polynomial of* $h \in R$: $h^* = \sum_i X^{k-i} \cdot h_i$

  $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
  $< X^i \cdot g, X^j \cdot h^* >= \theta^i((g \cdot h)_{k+j-i}) = 0$

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

  $h^*|_r X^n - 1/b$ *so* $C^\perp = (h^*)_{n,\theta,c}$

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.

- Proof
  1. *Let $C = (g)_{n,\theta}$ be a module θ-code of dimension k and let us assume that $C^{\perp}$ is a module θ-code.*

     $\exists p \in R, \deg(p) = k, C^{\perp} = (p)_{n,\theta}$

     $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
     $0 =< X^i \cdot g, X^j \cdot p > = \theta^i((g \cdot h)_{k+j-i})$ *with* $h = \theta^{-k}(p^*)$

     so $g \cdot h = X^n - b, b \in \mathbb{F}^*_{q^m}$

     and C is θ-constacyclic

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.

- Proof
  1. *Let $C = (g)_{n,\theta}$ be a module θ-code of dimension k and let us assume that $C^\perp$ is a module θ-code.*

     $\exists p \in R, \deg(p) = k, C^\perp = (p)_{n,\theta}$

     $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
     $0 = < X^i \cdot g, X^j \cdot p > = \theta^i((g \cdot h)_{k+j-i})$ *with* $h = \theta^{-k}(p^*)$

     so $g \cdot h = X^n - b, b \in \mathbb{F}_{q^m}^*$

     and C is θ-constacyclic

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.

- Proof
  1. *Let $C = (g)_{n,\theta}$ be a module θ-code of dimension k and let us assume that $C^\perp$ is a module θ-code.*

     $\exists p \in R, \deg(p) = k, C^\perp = (p)_{n,\theta}$

     $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
     $0 = < X^i \cdot g, X^j \cdot p > = \theta^i((g \cdot h)_{k+j-i})$ *with* $h = \theta^{-k}(p^*)$

     so $g \cdot h = X^n - b, b \in \mathbb{F}_{q^m}^*$

     and C is θ-constacyclic

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.

- Proof
  1. *Let $C = (g)_{n,\theta}$ be a module θ-code of dimension k and let us assume that $C^\perp$ is a module θ-code.*

     $\exists p \in R, \deg(p) = k, C^\perp = (p)_{n,\theta}$

     $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
     $0 =< X^i \cdot g, X^j \cdot p > = \theta^i((g \cdot h)_{k+j-i})$ *with* $h = \theta^{-k}(p^*)$

     so $g \cdot h = X^n - b, b \in \mathbb{F}_{q^m}^*$

     and C *is* θ*-constacyclic*

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.

- Proof
  1. *Let* $C = (g)_{n,\theta}$ *be a module* θ*-code of dimension* k *and let us assume that* $C^\perp$ *is a module* θ*-code.*

     $\exists p \in R, \deg(p) = k, C^\perp = (p)_{n,\theta}$

     $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
     $0 =< X^i \cdot g, X^j \cdot p > = \theta^i((g \cdot h)_{k+j-i})$ *with* $h = \theta^{-k}(p^*)$

     so $g \cdot h = X^n - b, b \in \mathbb{F}^*_{q^m}$

     and C *is* θ*-constacyclic*

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.

- Proof
  1. *Let $C = (g)_{n,\theta}$ be a module θ-code of dimension k and let us assume that $C^\perp$ is a module θ-code.*

     $\exists p \in R, \deg(p) = k, C^\perp = (p)_{n,\theta}$

     $\forall i \in \{0, \ldots, k-1\}, \forall j \in \{0, \ldots, n-k-1\}$
     $0 =< X^i \cdot g, X^j \cdot p > = \theta^i((g \cdot h)_{k+j-i})$ *with* $h = \theta^{-k}(p^*)$

     so $g \cdot h = X^n - b, b \in \mathbb{F}_{q^m}^*$

     and C is θ-constacyclic

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.
- Proof
  2. *Let $C = (g)_{n,\theta}$ be a shortened θ-constacyclic code.*

     Let $n' > n$ such that $C' = (g)_{n',\theta,c}$ be θ-constacyclic.

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.
- Proof
  2. *Let* $C = (g)_{n,\theta}$ *be a shortened* θ*-constacyclic code.*

     Let $n' > n$ *such that* $C' = (g)_{n',\theta,c}$ *be* θ*-constacyclic.*

     Let $c \in (\mathbb{F}_{q^m})^n$

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.
- Proof
  2. *Let* $C = (g)_{n,\theta}$ *be a shortened θ-constacyclic code.*

     Let $n' > n$ *such that* $C' = (g)_{n',\theta,c}$ *be θ-constacyclic.*

     Let $c \in (\mathbb{F}_{q^m})^n$
     $c \in C \quad \Leftrightarrow \quad (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in C'$

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.
- Proof
  2. *Let* $C = (g)_{n,\theta}$ *be a* *shortened θ-constacyclic* *code.*

     Let $n' > n$ *such that* $C' = (g)_{n',\theta,c}$ *be θ-constacyclic.*

     Let $c \in (\mathbb{F}_{q^m})^n$

     $$c \in C \quad \Leftrightarrow \quad (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in C'$$

     $$\Leftrightarrow \quad \forall c' \in C'^{\perp}, < (c_0, \ldots, c_{n-1}, 0, \ldots, 0), c' >= 0$$

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.
- Proof
  2. *Let* $C = (g)_{n,\theta}$ *be a shortened θ-constacyclic code.*

     Let $n' > n$ *such that* $C' = (g)_{n',\theta,c}$ *be θ-constacyclic.*

     Let $c \in (\mathbb{F}_{q^m})^n$

$$
\begin{aligned}
c \in C \quad & \Leftrightarrow \quad (c_0, \dots, c_{n-1}, 0, \dots, 0) \in C' \\
& \Leftrightarrow \quad \forall c' \in C'^{\perp}, < (c_0, \dots, c_{n-1}, 0, \dots, 0), c' >= 0 \\
& \Leftrightarrow \quad \forall c' \in C'^{\perp}, < c, \pi_{n' \to n}(c') >= 0
\end{aligned}
$$

Dual.

- The dual of a shortened θ-constacyclic code
  1. is not a module θ-code ;
  2. is a punctured code of a θ-constacyclic code.
- Proof
  2. *Let* $C = (g)_{n,\theta}$ *be a shortened* θ*-constacyclic code.*

     Let $n' > n$ *such that* $C' = (g)_{n',\theta,c}$ *be* θ*-constacyclic.*

     Let $c \in (\mathbb{F}_{q^m})^n$

$$\begin{aligned} c \in C \quad &\Leftrightarrow \quad (c_0, \ldots, c_{n-1}, 0, \ldots, 0) \in C' \\ &\Leftrightarrow \quad \forall c' \in C'^{\perp}, < (c_0, \ldots, c_{n-1}, 0, \ldots, 0), c' >= 0 \\ &\Leftrightarrow \quad \forall c' \in C'^{\perp}, < c, \pi_{n' \to n}(c') >= 0 \end{aligned}$$

     so $C^{\perp} = \pi_{n' \to n}(C'^{\perp})$

$R = \mathbb{F}_{q^m}[X;\theta]$, $\theta : a \mapsto a^q$

Module θ-code

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

θ-constacyclic

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

dual

θ-constacyclic

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

shortened θ-constacyclic

$C = \rho_{n' \to n}\left((g)_{n',\theta,c}\right)$

dual

punctured θ-constacyclic

$C^\perp = \pi_{n' \to n}\left((h^*)_{n',\theta,c}\right)$

Construction of self-dual module θ-codes.

- $C = (g)_{2k,\theta,c}$, $\deg(g) = k$
- $C = C^{\perp} \Leftrightarrow \forall i, j \in \{0, \ldots, k-1\}, < X^i \cdot g, X^j \cdot g >= 0$
- k^2 polynomial equations, k unknowns
- $N = \left\lfloor \frac{k}{2} \right\rfloor + 1$

  N polynomial equations, N unknowns

Construction of self-dual module θ-codes.

- $C = (g)_{2k,\theta,c}$, $\deg(g) = k$
- $C = C^{\perp} \Leftrightarrow \forall i, j \in \{0, \ldots, k-1\}, < X^i \cdot g, X^j \cdot g >= 0$
- k^2 polynomial equations, k unknowns
- $N = \left\lfloor \frac{k}{2} \right\rfloor + 1$

  N polynomial equations, N unknowns

Construction of self-dual module θ-codes.

- $C = (g)_{2k,\theta,c}$, $\deg(g) = k$
- $C = C^{\perp} \Leftrightarrow \forall i,j \in \{0,\ldots,k-1\}, < X^i \cdot g, X^j \cdot g >= 0$
- k^2 polynomial equations, k unknowns
- $N = \left\lfloor \frac{k}{2} \right\rfloor + 1$

  N polynomial equations, N unknowns

Construction of self-dual module θ-codes.

- $C = (g)_{2k,\theta,c}$, $\deg(g) = k$
- $C = C^{\perp} \Leftrightarrow \forall i, j \in \{0, \dots, k-1\}, < X^i \cdot g, X^j \cdot g >= 0$
- k^2 polynomial equations, k unknowns
- $N = \left\lfloor \frac{k}{2} \right\rfloor + 1$

  N polynomial equations, N unknowns

Construction over $\mathbb{F}_4$.

length	nbr pol	best distances	nbr of codes
4	3	3 - 3	1
6	3	3 - 3	1
8	**3**	**4** - 4	1
10	5	4 - 4	1
12	21	6 - 6	1
14	11	6 - 6	1
16	**3**	**4** - 6	1
18	27	6 - 6	2
20	63	8 - 8	1
22	33	8 - 8	1
24	93	7 - 8	2
26	65	8 - 8	3
28	279	9 - 9	4
30	285	10 - 10	1
32	**3**	**4** - 10	1
34	289	10 - 10	6
36	1 533	11 - 11	3
38	513	11 - 11	2
40	1 023	12 - 12	1

length	nbr pol	best distances	nbr of codes
42	2 211	12 - 12	21
44	3 171	14 - 14	1
46	2 051	14 - 14	1
48	1 533	12 - 14	18
50	5 125	14 - 14	4
52	12 483	14 - 14	41
54	13 851	14 - 14	47
56	18 051	15 - 15	2
58	16 385	15 - 15	9
60	136 269	16 - 16	5
62	42 875	17 - 17	1
64	**3**	**4** - 16	1
66	107 811	17 - 17	1
68	≥ 1	17 - 18	≥ 1
70	≥ 1	18 - 18	≥ 1
72	≥ 1	18 - 18	≥ 1
74	≥ 1	18 - 18	≥ 1
76	≥ 1	18 - 18	≥ 1
78	≥ 1	18 - 18	≥ 1

Gaborit, Otmani (2002) ; Grassl, Gulliver (2009) ; Chabot (2010) . . .

A family of self-dual θ-cyclic codes.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $s \geq 3$
- $g = (X+1)^{2^{s-1}}$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 2]_4$ θ-cyclic self-dual code
  single $[2^s, 2^{s-1}]_4$ cyclic code (self-dual)

- $g = (X+\alpha^i)\cdot(X+1)^{2^{s-1}-1}$, $i = 1, 2$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 4]_4$ self-dual θ-cyclic code

- Conjecture : there is no other $[2^s, 2^{s-1}]_4$ self-dual module θ-code.

A family of self-dual θ-cyclic codes.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $s \geq 3$
- $g = (X+1)^{2^{s-1}}$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 2]_4$ θ-cyclic self-dual code
  single $[2^s, 2^{s-1}]_4$ cyclic code (self-dual)

- $g = (X+\alpha^i) \cdot (X+1)^{2^{s-1}-1}$, $i = 1, 2$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 4]_4$ self-dual θ-cyclic code

- Conjecture : there is no other $[2^s, 2^{s-1}]_4$ self-dual module θ-code.

A family of self-dual θ-cyclic codes.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $s \geq 3$
- $g = (X+1)^{2^{s-1}}$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 2]_4$ θ-cyclic self-dual code
  single $[2^s, 2^{s-1}]_4$ cyclic code (self-dual)

- $g = (X+\alpha^i)\cdot(X+1)^{2^{s-1}-1}$, $i = 1, 2$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 4]_4$ self-dual θ-cyclic code

- Conjecture : there is no other $[2^s, 2^{s-1}]_4$ self-dual module θ-code.

A family of self-dual θ-cyclic codes.

- $\mathbb{F}_4 = \mathbb{F}_2(\alpha)$, $\theta : a \mapsto a^2$, $R = \mathbb{F}_4[X;\theta]$
- $s \geq 3$
- $g = (X+1)^{2^{s-1}}$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 2]_4$ θ-cyclic self-dual code
  single $[2^s, 2^{s-1}]_4$ cyclic code (self-dual)

- $g = (X+\alpha^i)\cdot(X+1)^{2^{s-1}-1}$, $i = 1, 2$

  $(g)_{2^s,\theta}$: $[2^s, 2^{s-1}, 4]_4$ self-dual θ-cyclic code

- Conjecture : there is no other $[2^s, 2^{s-1}]_4$ self-dual module θ-code.

A family of self-dual θ-cyclic codes.

- $C = (g)_{2^s,\theta}$, $g = (X + \alpha) \cdot (X + 1)^{2^{s-1}-1}$

1. C is θ-cyclic :

$$h = (X+1)^{2^{s-1}-1} \cdot (X + \alpha^2)$$
$$h \cdot g = (X+1)^{2^{s-1}-1} \cdot \underbrace{(X+\alpha^2) \cdot (X+\alpha)}_{X^2+1} \cdot (X+1)^{2^{s-1}-1} = X^{2^s} + 1 = g \cdot h$$

2. C is self-dual :

$$h^* = \alpha^2 g$$

3. Word of Hamming weight 4 :

$$m = (X+1)^{2^{s-2}-1} \cdot (X + \alpha^2)$$
$$m \cdot g = (X+1)^{2^{s-2}} \cdot (X+1)^{2^{s-1}} = X^{3\times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$$

- C, $[2^s, 2^{s-1},]_4$ self-dual θ-cyclic (noncyclic) code

A family of self-dual θ-cyclic codes.

- $C = (g)_{2^s,\theta}$, $g = (X+\alpha)\cdot(X+1)^{2^{s-1}-1}$

1. C is θ-cyclic :

$$h = (X+1)^{2^{s-1}-1}\cdot(X+\alpha^2)$$
$$h\cdot g = (X+1)^{2^{s-1}-1}\cdot\underbrace{(X+\alpha^2)\cdot(X+\alpha)}_{X^2+1}\cdot(X+1)^{2^{s-1}-1} = X^{2^s}+1 = g\cdot h$$

2. C is self-dual :

$$h^* = \alpha^2 g$$

3. Word of Hamming weight 4 :

$$m = (X+1)^{2^{s-2}-1}\cdot(X+\alpha^2)$$
$$m\cdot g = (X+1)^{2^{s-2}}\cdot(X+1)^{2^{s-1}} = X^{3\times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$$

- C, $[2^s, 2^{s-1},]_4$ self-dual θ-cyclic (noncyclic) code

A family of self-dual θ-cyclic codes.

- $C = (g)_{2^s,\theta}$, $g = (X+\alpha)\cdot(X+1)^{2^{s-1}-1}$

  1. C is θ-cyclic :

     $h = (X+1)^{2^{s-1}-1}\cdot(X+\alpha^2)$

     $h\cdot g = (X+1)^{2^{s-1}-1}\cdot\underbrace{(X+\alpha^2)\cdot(X+\alpha)}_{X^2+1}\cdot(X+1)^{2^{s-1}-1} = X^{2^s}+1 = g\cdot h$

  2. C is self-dual :

     $h^* = \alpha^2 g$

  3. Word of Hamming weight 4 :

     $m = (X+1)^{2^{s-2}-1}\cdot(X+\alpha^2)$

     $m\cdot g = (X+1)^{2^{s-2}}\cdot(X+1)^{2^{s-1}} = X^{3\times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$

- C, $[2^s, 2^{s-1},]_4$ self-dual θ-cyclic (noncyclic) code

A family of self-dual θ-cyclic codes.

- $C = (g)_{2^s,\theta}$, $g = (X+\alpha)\cdot(X+1)^{2^{s-1}-1}$

  1. C is θ-cyclic :
  $$h = (X+1)^{2^{s-1}-1}\cdot(X+\alpha^2)$$
  $$h\cdot g = (X+1)^{2^{s-1}-1}\cdot\underbrace{(X+\alpha^2)\cdot(X+\alpha)}_{X^2+1}\cdot(X+1)^{2^{s-1}-1} = X^{2^s}+1 = g\cdot h$$
  2. C is self-dual :
  $$h^* = \alpha^2 g$$
  3. Word of Hamming weight 4 :
  $$m = (X+1)^{2^{s-2}-1}\cdot(X+\alpha^2)$$
  $$m\cdot g = (X+1)^{2^{s-2}}\cdot(X+1)^{2^{s-1}} = X^{3\times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$$

- C, $[2^s, 2^{s-1},]_4$ self-dual θ-cyclic (noncyclic) code

A family of self-dual θ-cyclic codes.

- $C = (g)_{2^s,\theta}$, $g = (X+\alpha)\cdot(X+1)^{2^{s-1}-1}$

  1. C is θ-cyclic :
  $$h = (X+1)^{2^{s-1}-1}\cdot(X+\alpha^2)$$
  $$h\cdot g = (X+1)^{2^{s-1}-1}\cdot\underbrace{(X+\alpha^2)\cdot(X+\alpha)}_{X^2+1}\cdot(X+1)^{2^{s-1}-1} = X^{2^s}+1 = g\cdot h$$
  2. C is self-dual :
  $$h^* = \alpha^2 g$$
  3. Word of Hamming weight 4 :
  $$m = (X+1)^{2^{s-2}-1}\cdot(X+\alpha^2)$$
  $$m\cdot g = (X+1)^{2^{s-2}}\cdot(X+1)^{2^{s-1}} = X^{3\times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$$

- C, $[2^s, 2^{s-1}, \leq 4]_4$ self-dual θ-cyclic (noncyclic) code

A family of self-dual θ-cyclic codes.

- $C = (g)_{2^s,\theta}$, $g = (X+\alpha)\cdot(X+1)^{2^{s-1}-1}$

  1. C is θ-cyclic :
     $$h = (X+1)^{2^{s-1}-1}\cdot(X+\alpha^2)$$
     $$h\cdot g = (X+1)^{2^{s-1}-1}\cdot\underbrace{(X+\alpha^2)\cdot(X+\alpha)}_{X^2+1}\cdot(X+1)^{2^{s-1}-1} = X^{2^s}+1 = g\cdot h$$

  2. C is self-dual :
     $$h^* = \alpha^2 g$$

  3. Word of Hamming weight 4 :
     $$m = (X+1)^{2^{s-2}-1}\cdot(X+\alpha^2)$$
     $$m\cdot g = (X+1)^{2^{s-2}}\cdot(X+1)^{2^{s-1}} = X^{3\times 2^{s-2}} + X^{2^{s-1}} + X^{2^{s-2}} + 1$$

- C, $[2^s, 2^{s-1}, 4]_4$ self-dual θ-cyclic (noncyclic) code

Perspectives.

$$\theta \in Aut(\mathbb{F}_{q^m}),\ \alpha \in \mathbb{F}_{q^m},\ f = \sum_i f_i X^i \in \mathbb{F}_{q^m}[X;\theta]$$

- "Linear" evaluation

$$\mathcal{L}_f(\alpha) = \sum_i f_i \theta^i(\alpha)$$

$\longrightarrow$ Gabidulin codes (of linearized evaluation), Maximum Rank Distance

- "Polynomial" evaluation

$$f(\alpha) = Rem_r(f, X-\alpha) = \sum_i f_i \underbrace{N_i(\alpha)}_{\alpha\theta(\alpha)\ldots\theta^{i-1}(\alpha)}$$

$\longrightarrow$ "polynomial evaluation" skew codes

$\longrightarrow$ module and evaluation skew codes over $\mathbb{F}_{q^m}[X;\theta,\delta]$

Perspectives.

$$\theta \in Aut(\mathbb{F}_{q^m}),\ \alpha \in \mathbb{F}_{q^m},\ f = \sum_i f_i X^i \in \mathbb{F}_{q^m}[X;\theta]$$

- "Linear" evaluation

$$\mathcal{L}_f(\alpha) = \sum_i f_i \theta^i(\alpha)$$

$\longrightarrow$ Gabidulin codes (of linearized evaluation), Maximum Rank Distance

- "Polynomial" evaluation

$$f(\alpha) = Rem_r(f, X-\alpha) = \sum_i f_i \underbrace{N_i(\alpha)}_{\alpha\theta(\alpha)\ldots\theta^{i-1}(\alpha)}$$

$\longrightarrow$ "polynomial evaluation" skew codes

$\longrightarrow$ module and evaluation skew codes over $\mathbb{F}_{q^m}[X;\theta,\delta]$

Perspectives.

$$\theta \in Aut(\mathbb{F}_{q^m}),\ \alpha \in \mathbb{F}_{q^m},\ f = \sum_i f_i X^i \in \mathbb{F}_{q^m}[X;\theta]$$

- "Linear" evaluation

$$\mathcal{L}_f(\alpha) = \sum_i f_i \theta^i(\alpha)$$

$\longrightarrow$ Gabidulin codes (of linearized evaluation), Maximum Rank Distance

- "Polynomial" evaluation

$$f(\alpha) = Rem_r(f, X-\alpha) = \sum_i f_i \underbrace{N_i(\alpha)}_{\alpha\theta(\alpha)\ldots\theta^{i-1}(\alpha)}$$

$\longrightarrow$ "polynomial evaluation" skew codes

$\longrightarrow$ module and evaluation skew codes over $\mathbb{F}_{q^m}[X;\theta,\delta]$

Perspectives.

$$\theta \in Aut(\mathbb{F}_{q^m}),\ \alpha \in \mathbb{F}_{q^m},\ f = \sum_i f_i X^i \in \mathbb{F}_{q^m}[X;\theta]$$

- "Linear" evaluation

$$\mathcal{L}_f(\alpha) = \sum_i f_i \theta^i(\alpha)$$

$\longrightarrow$ Gabidulin codes (of linearized evaluation), Maximum Rank Distance

- "Polynomial" evaluation

$$f(\alpha) = Rem_r(f, X-\alpha) = \sum_i f_i \underbrace{N_i(\alpha)}_{\alpha\theta(\alpha)\ldots\theta^{i-1}(\alpha)}$$

$\longrightarrow$ "polynomial evaluation" skew codes

$\longrightarrow$ module and evaluation skew codes over $\mathbb{F}_{q^m}[X;\theta,\delta]$

Thank you for your attention !