Iterative decoding of $\theta-$cyclic codes.

Epiphane Nouetowa

IRMAR, Université de Rennes

Journées Nationales de calcul formel
March, 6th, 2024

Joint work with Ivan Pogildiakov

Let $\mathbb{F}_q$ be a finite field and $0 \leq k \leq n$ two positive integers.

Let $\mathbb{F}_q$ be a finite field and $0 \leq k \leq n$ two positive integers.

- A linear code C : $k-$dimensional subspace of $\mathbb{F}_q^n$.

Let $\mathbb{F}_q$ be a finite field and $0 \leq k \leq n$ two positive integers.

- A linear code C : $k-$dimensional subspace of $\mathbb{F}_q^n$.
- The minimum distance of C is

$$d = \min_{c \in C, c \neq 0} \{w_H(c)\}$$

where $w_H(c) = \#\{i, c_i \neq 0\}$.

Let $\mathbb{F}_q$ be a finite field and $0 \leq k \leq n$ two positive integers.

- A linear code C : $k-$dimensional subspace of $\mathbb{F}_q^n$.
- The minimum distance of C is

$$d = \min_{c \in C, c \neq 0} \{w_H(c)\}$$

  where $w_H(c) = \#\{i, c_i \neq 0\}$.
- The **Euclidean dual** of C is

$$C^{\perp} = \{x \in \mathbb{F}_q^n / \forall c \in C, < x, c >= 0\}$$

  where $<,>$ is the Euclidean inner product over $\mathbb{F}_q^n$.

Let $\mathbb{F}_q$ be a finite field and $0 \leq k \leq n$ two positive integers.

- A linear code C : $k-$dimensional subspace of $\mathbb{F}_q^n$.
- The minimum distance of C is

$$d = \min_{c \in C, c \neq 0} \{w_H(c)\}$$

  where $w_H(c) = \#\{i, c_i \neq 0\}$.
- The **Euclidean dual** of C is

$$C^{\perp} = \{x \in \mathbb{F}_q^n / \forall c \in C, < x, c >= 0\}$$

  where $<,>$ is the Euclidean inner product over $\mathbb{F}_q^n$.

- Notation: $C : [n, k, d]_q$.

The $[n, k, d]_q$ code is a **cyclic code** if

$$\forall c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}, (c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$$

The $[n, k, d]_q$ code is a **cyclic code** if

$$\forall c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}, (c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$$

Let $\theta \in Aut(\mathbb{F}_q)$ be an automorphism over $\mathbb{F}_q$.

The $[n, k, d]_q$ code is a **cyclic code** if

$$\forall c = (c_0, \ldots, c_{n-1}) \in \mathcal{C}, (c_{n-1}, c_0, \cdots, c_{n-2}) \in \mathcal{C}$$

Let $\theta \in Aut(\mathbb{F}_q)$ be an automorphism over $\mathbb{F}_q$.

Definition 1 (Boucher, Geiselmann and Ulmer 2007)

A $\theta-$**cyclic code** of length n over $\mathbb{F}_q$ is a linear code $\mathcal{C}$ defined by: $\forall (c_0, c_1, \ldots, c_{n-1}) \in \mathbb{F}_q^n$,

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

Aim : Designing an iterative decoding algorithm for $\theta-$cyclic codes.

J. Xing, M. Bossert, S. Bitzer and L. Chen, *Iterative Decoding of Non-Binary Cyclic Codes Using Minimum-Weight Dual Codewords*, ISIT(2020)

Tool : skew polynomials and duality.

Let $\theta \in Aut(\mathbb{F}_q)$.

Skew polynomial ring: $\mathbb{F}_q[x;\theta] = \left\{ \sum_{i=0}^{n} a_i x^i \mid a_i \in \mathbb{F}_q, n \in \mathbb{N} \right\}$

where the multiplication is defined by

$$x.a = \theta(a)x, \forall a \in \mathbb{F}_q.$$

$\mathbb{F}_q[x;\theta]$ is right and left Euclidean.

- For $c = (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$ we denote $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x; \theta]$.

- For $c = (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$ we denote $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x; \theta]$.
- For $C \subset \mathbb{F}_q^n$ we denote $C(x) = \{c(x) \mid c \in C\}$.

- For $c = (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$ we denote $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x; \theta]$.
- For $C \subset \mathbb{F}_q^n$ we denote $C(x) = \{c(x) \mid c \in C\}$.
- $[n, k, d]_q$ θ-cyclic code $\mathcal{C}$

$$\mathcal{C}(x) = \{m(x)g(x) \mid m(x) \in \mathbb{F}_q[x; \theta], \deg(m(x)) < k\}$$

where $g(x)$ is a right divisor of $x^n - 1$ and $\deg(g(x)) = n - k$.

- For $c = (c_0, ..., c_{n-1}) \in \mathbb{F}_q^n$ we denote $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \mathbb{F}_q[x; \theta]$.
- For $C \subset \mathbb{F}_q^n$ we denote $C(x) = \{c(x) \mid c \in C\}$.
- $[n, k, d]_q$ θ-cyclic code $\mathcal{C}$

$$\mathcal{C}(x) = \{m(x)g(x) \mid m(x) \in \mathbb{F}_q[x; \theta], \deg(m(x)) < k\}$$

where $g(x)$ is a right divisor of $x^n - 1$ and $\deg(g(x)) = n - k$.

- Notation: $\mathcal{C} = (g)_{n,\theta}$

Assume that the order of θ divides n.

The **skew reciprocal** of $h(x) = \sum_{i=0}^{k} h_i x^i \in \mathbb{F}_q[x;\theta]$ is

$$h^*(x) = \sum_{i=0}^{k} x^{k-i} h_i = \sum_{i=0}^{k} \theta^{k-i}(h_i) x^{k-i}.$$

Proposition 1

*The **Euclidean dual** of $\mathcal{C} = (g)_{n,\theta}$ is*

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

where $x^n - 1 = h(x)g(x)$.

The **skew reciprocal** of $h(x) = \sum_{i=0}^{k} h_i x^i \in \mathbb{F}_q[x;\theta]$ is

$$h^*(x) = \sum_{i=0}^{k} x^{k-i} h_i = \sum_{i=0}^{k} \theta^{k-i}(h_i) x^{k-i}.$$

Proposition 1

*The **Euclidean dual** of $\mathcal{C} = (g)_{n,\theta}$ is*

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

where $x^n - 1 = h(x)g(x)$.

Remark 1

$x^n - 1 = h(x)g(x) = g(x)h(x)$

Example

$\theta : \alpha \mapsto \alpha^2 \in Aut(\mathbb{F}_4)$, where $\mathbb{F}_4 = \mathbb{F}_2(a)$ with $a^2 + a + 1 = 0$.

$$x^{12} - 1 = (\underbrace{x^4 + a^2x^2 + x + a^2}_{h(x)})(\underbrace{x^8 + a^2x^6 + x^5 + x^4 + x^3 + x + a}_{g(x)})$$

$\mathcal{C} = (g)_{12,\theta} : [12, 4, 7]_4$

$\mathcal{C}^{\perp} = (h^*)_{12,\theta} : [12, 8, 4]_4$ with $h^*(x) = a^2x^4 + x^3 + a^2x^2 + 1$

$c(x) = (x^3 + a^2x^2 + x + a)g(x) \in \mathcal{C}(x)$

Notation: For $h(x) = \sum_{i=0}^{k} h_i x^i \in \mathbb{F}_q[x;\theta]$, one denotes $\theta(h(x)) = \sum_{i=0}^{k} \theta(h_i) x^i$.

Proposition 2

Consider $c \in \mathcal{C} = (g)_{n,\theta}$ *and* $u \in \mathcal{C}^{\perp} = (h^*)_{n,\theta}$

$$c(x)\theta^{-\ell}(u^*(x)) = 0 \bmod (x^n - 1)$$

where $\ell = \deg(u(x))$.

Proof

Consider $c \in \mathcal{C} = (g)_{n,\theta}$, $u \in \mathcal{C}^{\perp} = (h^*)_{n,\theta}$ and $\ell = \deg(u^*(x))$.
One has $c(x) = v(x)g(x)$ and $u(x) = m(x)h^*(x)$.

Furthermore $u^*(x) = \theta^{\deg(m(x))}(h^{**}(x))m^*(x)$ and $h^{**}(x) = \theta^{\deg(h(x))}(h(x))$.

Therefore $u^*(x) = \theta^{\ell}(h(x))m^*(x)$ and $\theta^{-\ell}(u^*(x)) = h(x)\theta^{-\ell}(m^*(x))$.

$$\begin{aligned} c(x)\theta^{-\ell}(u^*(x)) &= v(x)g(x)h(x)\theta^{-\ell}(m^*(x)) \\ &= v(x)(x^n-1)\theta^{-\ell}(m^*(x)) \\ &= v(x)\theta^{-\ell}(m^*(x))(x^n-1) \\ &\equiv 0 \bmod (x^n-1) \end{aligned}$$

Assume that we received $y(x) = c(x) + e(x)$ with $c \in \mathcal{C}$, $w_H(e) \leq \tau$. We want to find $e(x)$.

Corollary 1

Consider $f(x) = \theta^{-\ell}(u^*(x))$, where $u \in \mathcal{C}^{\perp}$ and $\ell = \deg(u(x))$. On has

$$y(x)f(x) \equiv e(x)f(x) \bmod (x^n - 1)$$

$$y(x)f(x) \equiv c(x)f(x) + e(x)f(x) \bmod (x^n - 1)$$

Definition 2

Two words c_1 and $c_2 \in \mathbb{F}_q^n$ are $\theta-$**cyclically equivalent** if there exist $b \in \mathbb{F}_q$ and $i \in \mathbb{N}$ such that $c_2 = b\psi^i(c_1)$ where

$$\psi : \begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (v_0, ..., v_{n-1}) & \longmapsto & (\theta(v_{n-1}), \theta(v_0), \ldots, \theta(v_{n-2})). \end{cases}$$

Definition 2

Two words c_1 and $c_2 \in \mathbb{F}_q^n$ are $\theta-$**cyclically equivalent** if there exist $b \in \mathbb{F}_q$ and $i \in \mathbb{N}$ such that $c_2 = b\psi^i(c_1)$ where

$$\psi : \begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (v_0, ..., v_{n-1}) & \longmapsto & (\theta(v_{n-1}), \theta(v_0), \ldots, \theta(v_{n-2})). \end{cases}$$

Let $\nu \in \mathbb{Z}_{>0}$ such that there is $u \in \mathcal{C}^{\perp}, w_H(u) = \nu$.

Definition 2

Two words c_1 and $c_2 \in \mathbb{F}_q^n$ are $\theta-$**cyclically equivalent** if there exist $b \in \mathbb{F}_q$ and $i \in \mathbb{N}$ such that $c_2 = b\psi^i(c_1)$ where

$$\psi : \begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (v_0, ..., v_{n-1}) & \longmapsto & (\theta(v_{n-1}), \theta(v_0), \ldots, \theta(v_{n-2})). \end{cases}$$

Let $\nu \in \mathbb{Z}_{>0}$ such that there is $u \in \mathcal{C}^{\perp}, w_H(u) = \nu$.

$$\mathcal{B}_\nu := \{u(x) \text{ monic and } \theta-\text{cyclically different} | u \in \mathcal{C}^{\perp}, w_H(u) = \nu\}$$

Definition 2

Two words c_1 and $c_2 \in \mathbb{F}_q^n$ are $\theta-$**cyclically equivalent** if there exist $b \in \mathbb{F}_q$ and $i \in \mathbb{N}$ such that $c_2 = b\psi^i(c_1)$ where

$$\psi : \begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (v_0, ..., v_{n-1}) & \longmapsto & (\theta(v_{n-1}), \theta(v_0), \ldots, \theta(v_{n-2})). \end{cases}$$

Let $\nu \in \mathbb{Z}_{>0}$ such that there is $u \in \mathcal{C}^\perp, w_H(u) = \nu$.

$$\mathcal{B}_\nu := \{u(x) \text{ monic and } \theta-\text{cyclically different} | u \in \mathcal{C}^\perp, w_H(u) = \nu\}$$

$$\overline{\mathcal{B}}_\nu := \{\theta^{-\ell}(u^*(x)) | u(x) \in \mathcal{B}_\nu, \ell = \deg(u(x))\}$$

.

Definition 2

Two words c_1 and $c_2 \in \mathbb{F}_q^n$ are $\theta-$**cyclically equivalent** if there exist $b \in \mathbb{F}_q$ and $i \in \mathbb{N}$ such that $c_2 = b\psi^i(c_1)$ where

$$\psi : \begin{cases} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (v_0, ..., v_{n-1}) & \longmapsto & (\theta(v_{n-1}), \theta(v_0), \ldots, \theta(v_{n-2})). \end{cases}$$

Let $\nu \in \mathbb{Z}_{>0}$ such that there is $u \in \mathcal{C}^\perp, w_H(u) = \nu$.

$$\mathcal{B}_\nu := \{u(x) \text{ monic and } \theta-\text{cyclically different} | u \in \mathcal{C}^\perp, w_H(u) = \nu\}$$

$$\overline{\mathcal{B}}_\nu := \{\theta^{-\ell}(u^*(x)) | u(x) \in \mathcal{B}_\nu, \ell = \deg(u(x))\}$$

.

Remark 2

$f(x) \in \overline{\mathcal{B}}_\nu$ *has the form* $1 + \lambda_{\beta_1} x^{\beta_1} + \ldots + \lambda_{\beta_{\nu-1}} x^{\beta_{\nu-1}}$.

Example (continued)

$\overline{\mathcal{B}}_4 = \{1 + x^3 + x^6 + x^9, 1 + a^2x + x^2 + ax^4, 1 + a^2x^2 + a^2x^4 + x^9, 1 + x + a^2x^3 + ax^8, 1 + x^4 + x^6 + x^{10}, 1 + a^2x^3 + ax^4 + x^5, 1 + x + x^6 + x^7, 1 + ax + x^4 + ax^9\}$.

Let $e(x) = a^2x^{11} + ax^7 + x^2$ be an error.

Example (continued)

$\overline{\mathcal{B}}_4 = \{1 + x^3 + x^6 + x^9, 1 + a^2x + x^2 + ax^4, 1 + a^2x^2 + a^2x^4 + x^9, 1 + x + a^2x^3 + ax^8, 1 + x^4 + x^6 + x^{10}, 1 + a^2x^3 + ax^4 + x^5, 1 + x + x^6 + x^7, 1 + ax + x^4 + ax^9\}$.

Let $e(x) = a^2x^{11} + ax^7 + x^2$ be an error.

- For $f(x) = 1 + ax + x^4 + ax^9 \in \overline{\mathcal{B}}_4$, one has

$$e(x)f(x) \bmod (x^{12} - 1) = a^2x^{11} + a^2x^8 + ax^7 + x^6 + x^4 + x^3 + x^2 + a$$

Example (continued)

$\overline{\mathcal{B}}_4 = \{1 + x^3 + x^6 + x^9, 1 + a^2x + x^2 + ax^4, 1 + a^2x^2 + a^2x^4 + x^9, 1 + x + a^2x^3 + ax^8, 1 + x^4 + x^6 + x^{10}, 1 + a^2x^3 + ax^4 + x^5, 1 + x + x^6 + x^7, 1 + ax + x^4 + ax^9\}$.

Let $e(x) = a^2x^{11} + ax^7 + x^2$ be an error.

- For $f(x) = 1 + ax + x^4 + ax^9 \in \overline{\mathcal{B}}_4$, one has

$$e(x)f(x) \bmod (x^{12} - 1) = a^2x^{11} + a^2x^8 + ax^7 + x^6 + x^4 + x^3 + x^2 + a$$

- For $f(x) = 1 + x + a^2x^3 + ax^8 \in \overline{\mathcal{B}}_4$, one has

$$e(x)f(x) \bmod (x^{12} - 1) = a^2x^{11} + x^{10} + ax^8 + a^2x^5 + a^2$$

Example (continued)

$\overline{\mathcal{B}}_4 = \{1 + x^3 + x^6 + x^9, 1 + a^2x + x^2 + ax^4, 1 + a^2x^2 + a^2x^4 + x^9, 1 + x + a^2x^3 + ax^8, 1 + x^4 + x^6 + x^{10}, 1 + a^2x^3 + ax^4 + x^5, 1 + x + x^6 + x^7, 1 + ax + x^4 + ax^9\}$.

Let $e(x) = a^2x^{11} + ax^7 + x^2$ be an error.

- For $f(x) = 1 + ax + x^4 + ax^9 \in \overline{\mathcal{B}}_4$, one has

$$e(x)f(x) \bmod (x^{12} - 1) = a^2x^{11} + a^2x^8 + ax^7 + x^6 + x^4 + x^3 + x^2 + a$$

- For $f(x) = 1 + x + a^2x^3 + ax^8 \in \overline{\mathcal{B}}_4$, one has

$$e(x)f(x) \bmod (x^{12} - 1) = a^2x^{11} + x^{10} + ax^8 + a^2x^5 + a^2$$

$$e(x)f(x)a^2x^9 \bmod (x^{12} - 1) = ax^9 + x^8 + a^2x^7 + x^5 + x^2$$

Assume that we received $y(x) = c(x) + e(x)$ with $c \in \mathcal{C}$, $w_H(e) \leq \tau$.

- For $f(x) \in \overline{\mathcal{B}}_\nu$,

$$\begin{aligned} w_f^0(x) &:= y(x)f(x) \bmod (x^n - 1) \\ &= e(x) + e(x)\lambda_{\beta_1}x^{\beta_1} + \ldots + e(x)\lambda_{\beta_{\nu-1}}x^{\beta_{\nu-1}} \bmod (x^n - 1). \end{aligned}$$

Assume that we received $y(x) = c(x) + e(x)$ with $c \in \mathcal{C}$, $w_H(e) \leq \tau$.

- For $f(x) \in \overline{\mathcal{B}}_\nu$,

$$\begin{aligned} w_f^0(x) &:= y(x)f(x) \bmod (x^n - 1) \\ &= e(x) + e(x)\lambda_{\beta_1}x^{\beta_1} + \ldots + e(x)\lambda_{\beta_{\nu-1}}x^{\beta_{\nu-1}} \bmod (x^n - 1). \end{aligned}$$

- For $i \in \{1, \ldots, \nu - 1\}$,

$$w_f^i(x) := w_f^0(x)\theta^{n-\beta_i}\left(\lambda_{\beta_i}^{-1}\right)x^{n-\beta_i} \bmod (x^n - 1).$$

Assume that we received $y(x) = c(x) + e(x)$ with $c \in \mathcal{C}$, $w_H(e) \leq \tau$.

- For $f(x) \in \overline{\mathcal{B}}_\nu$,

$$\begin{aligned} w_f^0(x) &:= y(x)f(x) \bmod (x^n - 1) \\ &= e(x) + e(x)\lambda_{\beta_1}x^{\beta_1} + \ldots + e(x)\lambda_{\beta_{\nu-1}}x^{\beta_{\nu-1}} \bmod (x^n - 1). \end{aligned}$$

- For $i \in \{1, \ldots, \nu - 1\}$,

$$w_f^i(x) := w_f^0(x)\theta^{n-\beta_i}\left(\lambda_{\beta_i}^{-1}\right)x^{n-\beta_i} \bmod (x^n - 1).$$

- For $\alpha \in \mathbb{F}_q$ and $j \in \{0, \ldots, n-1\}$,

$$\mathcal{T}(\alpha, j) := \#\{w_f^i \mid i \in \{0, \ldots, \nu - 1\}, f(x) \in \overline{\mathcal{B}}_\nu \text{ and } (w_f^i)_j = \alpha\}.$$

Example (continued)

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 1

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^7 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	2	3	4	5	6	7	8	9	10	11
0	11	11	3	13	11	8	14	2	10	14	12	3
1	7	5	17	9	9	6	6	4	8	6	6	5
a	7	11	7	5	7	8	6	18	6	6	8	7
a^2	7	5	5	5	5	10	6	8	8	6	6	17

Example (continued)

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 1

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^7 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	2	3	4	5	6	**7**	8	9	10	11
0	11	11	3	13	11	8	14	2	10	14	12	3
1	7	5	17	9	9	6	6	4	8	6	6	5
a	7	11	7	5	7	8	6	18	6	6	8	7
a^2	7	5	5	5	5	10	6	8	8	6	6	17

Example (continued)

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 1

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^7 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	2	3	4	5	6	**7**	8	9	10	11
0	11	11	3	13	11	8	14	**2**	10	14	12	3
1	7	5	17	9	9	6	6	**4**	8	6	6	5
a	7	11	7	5	7	8	6	**18**	6	6	8	7
a^2	7	5	5	5	5	10	6	**8**	8	6	6	17

Example (continued)

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 1

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^7 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	2	3	4	5	6	**7**	8	9	10	11
0	11	11	3	13	11	8	14	**2**	10	14	12	3
1	7	5	17	9	9	6	6	**4**	8	6	6	5
a	7	11	7	5	7	8	6	**18**	6	6	8	7
a^2	7	5	5	5	5	10	6	**8**	8	6	6	17

Example (continued)

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 1

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^7 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	2	3	4	5	6	**7**	8	9	10	11
0	11	11	3	13	11	8	14	**2**	10	14	12	3
1	7	5	17	9	9	6	6	**4**	8	6	6	5
a	7	11	7	5	7	8	6	**18**	6	6	8	7
a^2	7	5	5	5	5	10	6	**8**	8	6	6	17

Example (continued)

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 1

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^7 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	2	3	4	5	6	**7**	8	9	10	11
0	11	11	3	13	11	8	14	**2**	10	14	12	3
1	7	5	17	9	9	6	6	**4**	8	6	6	5
a	7	11	7	5	7	8	6	**18**	6	6	8	7
a^2	7	5	5	5	5	10	6	**8**	8	6	6	17

$$y(x) \leftarrow y(x) - \mathbf{a}x^7$$

One checks that $y(x) \notin \mathcal{C}$.

$$e(x) = a^2x^{11} + ax^7 + x^2$$

Step 2

$$y(x) = ax^{11} + a^2x^{10} + a^2x^9 + x^8 + ax^6 + ax^4 + ax^3 + x^2 + x + a^2$$

	0	1	**2**	3	4	5	6	7	8	9	10	**11**
0	16	19	**2**	18	16	14	19	18	14	19	19	**2**
1	6	5	**22**	8	6	2	5	8	10	5	5	**2**
a	4	3	**6**	2	4	6	3	2	6	3	3	**6**
$\mathbf{a^2}$	6	5	**2**	4	6	10	5	4	2	5	5	**22**

$$y(x) \leftarrow y(x) - (\mathbf{1}x^2 + \mathbf{a^2}x^{11})$$

One checks that $y(x) \in \mathcal{C}$.

Implementation in C and experimentations over $\mathbb{F}_4$ and $\mathbb{F}_9$. 100 000 tests for each error weight.

Codes	$[54, 27, 18]_9$		$[54, 19, 21]_9$		$[62, 26, 19]_4$	
Duals	$[54, 27, 18]_9$		$[54, 35, 6]_9$		$[62, 36, 13]_4$	
ν	18		13		13	
Success rate	$\tau \leq 7$	1	$\tau \leq 12$	1	$\tau \leq 7$	1
	$\tau = 8$	$0,9923$	$\tau = 13$	$0,9999$	$\tau = 8$	$0,9878$
	$\tau = 9$	$0,7532$	$\tau = 14$	$0,9918$	$\tau = 9$	$0,8346$

Consider $f(x) = 1 + \lambda_{\beta_1} x^{\beta_1} + \ldots + \lambda_{\beta_{\nu-1}} x^{\beta_{\nu-1}}$ in $\mathbb{F}_q[x;\theta]$, the support S_f^0 of $f(x)$:

$$S_f^0 := \{0, \beta_1, \ldots, \beta_{\nu-1}\}$$

and for $0 < i < \nu$ we denote S_f^i the support of $f(x)\theta^{-\beta_i}\left(\lambda_{\beta_i}^{-1}\right) x^{n-\beta_i} \bmod (x^n - 1)$:

$$S_f^i := \{v - \beta_i \bmod n, v \in S_f^0\}.$$

Consider

$$\mathcal{I} = \bigcap_{i=0, f \in \overline{\mathcal{B}}_\nu}^{\nu-1} S_f^i$$

Lemma 3

If the weight of e is equal to 1, then the algorithm is successful if and only if $\mathcal{I} = \{0\}$.

Conjecture: If $\mathcal{I} \neq \{0\}$, the iterative decoding Algorithm returns Failure.

Some questions are in order.

- How to choose ν ?
- How many elements in $\overline{\mathcal{B}}_\nu$?
- Given ν how can we compute efficiently the words of weight ν for a θ-cyclic code ?

Thank you!