Iterative decoding of $\theta-$cyclic codes.

Epiphane Nouetowa and Ivan Pogildiakov

IRMAR, Université de Rennes

Journées C2
October, 17th, 2023

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

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

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

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

We will be using the usual convention :

$$c = (c_0, \ldots, c_{n-1}) \in \mathbb{F}_q^n \leftrightarrow c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{F}_q[x; \theta].$$

Definition 1

A $\theta-$**cyclic code** $\mathcal{C}$ of length n and dimension k over $\mathbb{F}_q$ is defined by:

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

where $g(x)$ is a right divisor of $x^n - 1$ with degree $n - k$.

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

The dual of $\mathcal{C}$ is

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

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

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 $h^*(x) = a^2x^4 + x^3 + a^2x^2 + 1$

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

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

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

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

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

.

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

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

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

- For $i \in \{1, \ldots, d^\perp - 1\}$,

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

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

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

Example

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

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

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

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

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

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

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

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

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

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

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

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
a^2	6	5	2	4	6	10	5	4	2	5	5	22

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

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

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

$\mathcal{C}$: $[54, 27, 18]_9$ $\mathcal{C}^\perp$: $[54, 27, 18]_9$		$\mathcal{C}$: $[54, 19, 21]_9$ $\mathcal{C}^\perp$: $[54, 35, 6]_9$	
$w_H(e)$	success	$w_H(e)$	success
7	100%	7	100%
8	99,23%	8	100%
9	75,32%	9	100%
		10	100%
		11	100%
		12	100%
		13	99,99%

Thank you!