CYCLIC CODES AS HYPERINVARIANT SUBSPACES

M. Isabel García-Planas
Dept. de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Spain
maria.isabel.garcia@upc.edu

M. Dolors Magret
Dept. de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Spain
m.dolors.magret@upc.edu

M. Eulalia Montoro
Dept. de Matemàtica Aplicada I
Universitat Politècnica de Catalunya
Spain
maria.eulalia.montoro@upc.edu

Abstract

It is known the relationship between cyclic codes and invariant subspaces. We present in this work some codes which are obtained from invariant and hyperinvariant subspaces of the linear maps having associated matrices, in the standard basis, of a special form.

Key words

Cyclic codes, hyperinvariant subspaces.

1 Introduction

Let φ be an endomorphism of a vector space V over a field $\mathbb{F}$. A φ-invariant subspace $F \subset V$ is called hyperinvariant if F is invariant under all linear maps commuting with φ.

The main goal of this work is to regard some kind of codes as invariant linear subspaces of $\mathbb{F}^n$ with respect to α, β cyclic shift map over a position, Despite the commutative algebra is the tool normally used to study linear cyclic codes (see [MacWilliams, Sloane, 1977], for example) the linear codes have a structure of linear subspaces of $\mathbb{F}^n$, then is natural to describe linear codes in terms of linear algebra.

2 Preliminaries

Let $\mathbb{F} = GF(q)$ be a finite field of q elements, $q = p^k$, p a prime number and let $\mathbb{F}^n$ be the n-dimensional vector space over the field $\mathbb{F}$. We consider the standard basis $e_i = (0,\dots 0, \underset{\check{i}}{1}, 0, \dots, 0)$, for $i = 1, \dots, n$.

We consider the following linear map

$$\begin{aligned} \varphi : \mathbb{F}^n &\longrightarrow \mathbb{F}^n \\ (x_1, \dots, x_n) &\longrightarrow (x_n, x_1, \dots, x_{n-1}) \end{aligned} \tag{1}$$

with associated matrix with respect to the standard basis,

$$A = \begin{pmatrix} 0\,0 \dots 0\,1 \\ 1\,0 \dots 0\,0 \\ 0\,1 \dots 0\,0 \\ \vdots\ \vdots \ddots \vdots\ \vdots \\ 0\,0 \dots 1\,0 \end{pmatrix}. \tag{2}$$

This linear map is clearly orthogonal ($A^t = A^{-1}$) and verifies $A^n = I_n$. Cayley Hamilton Theorem ensures that the characteristic polynomial is

$$p(s) = \det(A - sI_n) = (-1)^n(s^n - 1).$$

In order to obtain the hyperinvariant subspaces we need to compute the centralizer of the linear map A.

Proposition 2.1. *The centralizer $\mathcal{C}(A)$ of A is the set of circulant matrices*

$$X = \begin{pmatrix} x_1 & x_2 & \dots & x_{n-1} & x_n \\ x_n & x_1 & \dots & x_{n-2} & x_{n-1} \\ x_{n-1} & x_n & \dots & x_{n-3} & x_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2 & x_3 & \dots & x_n & x_1 \end{pmatrix}$$

Proof. It suffices to solve the matrix equation $AX - XA = 0$.

Remark 2.1. *If X is any circulant matrix of order n, then the centralizer of X is $\mathcal{C}(A)$. That is to say, two circulant matrices of the same order commute.*

Definition 2.1. *If $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$ are two vectors in $\mathbb{F}^n$, we will say that x and y are orthogonal when $x \cdot y^t = 0$.*

Remark 2.2. *Notice that $X \in \mathcal{C}(A)$ if, and only if, $X^t \in \mathcal{C}(A)$. In particular all circulant matrices are normal matrices (in the sense that $XX^t = X^tX$), and we have the following Proposition.*

Proposition 2.2. *If F is an hyperinvariant subspace of φ, then $F^{\perp}$ is also hyperinvariant.*

Proof. Given any $w \in F^{\perp}$, $c \in F$, $X \in \mathcal{C}(A)$, if $(w')^t = X^t w^t$ then taking into account 2.2 we have:

$$w'c^t = wXc^t = 0$$

and then $w' \in F^{\perp}$ and $F^{\perp}$ is hyperinvariant.

Notice that if $v = (v_1, \dots, v_n)$ is an eigenvector of A, then the following equalities hold:

$$\begin{aligned} v_n &= \lambda v_1 \\ v_1 &= \lambda v_2 \\ &\dots \\ v_{n-2} &= \lambda v_{n-1} \\ v_{n-1} &= \lambda v_n \end{aligned} \tag{3}$$

In particular, we obtain that

$$v = (\lambda^{n-1}, \lambda^{n-2}, \dots, \lambda, 1)$$

and we have the following Proposition

Proposition 2.3. *Given any $\lambda \in GF(q)^*$ such that $\lambda^n = 1$, then $[v]$ with $v = (\lambda^{n-1}, \lambda^{n-2}, \dots, \lambda, 1)$ is an hyperinvariant subspace.*

Corollary 2.1. *The subspace $F = [(1, 1, \dots, 1, 1)]$ is hyperinvariant.*

The Euler-Fermat Theorem provides information about the roots of $\lambda^n - 1$.

Theorem 2.1. *If $\mathbb{F} = GF(q)$, then $\lambda^{q-1} = 1$ has $q - 1$ different roots.*

Example 2.1. *Consider $n = 4$ and $\mathbb{F} = GF(5)$. In this case, as a consequence of Euler-Fermat Theorem, the characteristic polynomial has four different roots. In particular the eigenvalues of A are $\lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_3 = 3$, $\lambda_4 = 4$.*

The subspace G=[(3,4,2,1)] is A-invariant:

$$\begin{pmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 2 \\ 1 \end{pmatrix} = 2 \begin{pmatrix} 3 \\ 4 \\ 2 \\ 1 \end{pmatrix}$$

and G is also hyperinvariant because

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_1 & x_2 & x_3 \\ x_3 & x_4 & x_1 & x_2 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 2 \\ 1 \end{pmatrix} = (3x_2 + 4x_3 + 2x_4 + x_1) \begin{pmatrix} 3 \\ 4 \\ 2 \\ 1 \end{pmatrix}$$

The subspace H=[(1,4,1,4)] is A-invariant:

$$\begin{pmatrix} 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 1 \\ 4 \end{pmatrix} = 4 \begin{pmatrix} 1 \\ 4 \\ 1 \\ 4 \end{pmatrix}$$

and H is also hyperinvariant because

$$\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_1 & x_2 & x_3 \\ x_3 & x_4 & x_1 & x_2 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 1 \\ 4 \end{pmatrix} = (x_1 + 4x_2 + x_3 + 4x_4) \begin{pmatrix} 1 \\ 4 \\ 1 \\ 4 \end{pmatrix}.$$

In general we have the following result.

Proposition 2.4. *Let v an eigenvector of A corresponding to the simple eigenvalue α. Then v is an eigenvector of X for all $X \in \mathcal{C}(A)$.*

Proof. As a consequence of the definitions,

$$AXv = XAv = X\alpha v = \alpha Xv,$$

then Xv is the zero vector or it is an eigenvector of A of eigenvalue α for all $X \in \mathcal{C}(A)$.

Taking into account that α is simple we have that $Xv = \lambda v$, and the proof is completed.

We can compute the value of the eigenvalue as follows.

Let v be an eigenvector of A corresponding to the eigenvalue α. Taking into account that $v \neq 0$ we can consider $v = (v_1, \dots, v_{i-1}, 1, v_{i+1}, \dots, v_n)$.

$$\begin{pmatrix} x_1 & x_2 & \dots & x_{n-1} & x_n \\ x_n & x_1 & \dots & x_{n-2} & x_{n-1} \\ x_{n-1} & x_n & \dots & x_{n-3} & x_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_2 & x_3 & \dots & x_n & x_1 \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ 1 \\ \vdots \\ v_n \end{pmatrix} = \lambda \begin{pmatrix} v_1 \\ \vdots \\ 1 \\ \vdots \\ v_n \end{pmatrix}$$

The i-th coordinate of Xv is $x_{n-i+2}v_1 + \dots + x_{n-i+1}v_n = \lambda$.

Not only one dimensional invariant subspaces are hyperinvariant, but invariant subspaces are also hyperinvariants.

Proposition 2.5. *Let F be an invariant subspace of A. Then it is hyperinvariant.*

Proof. It suffices to observe that, for all $X \in \mathcal{C}(A)$ then

$$X = x_1 I + x_2 A^{n-1} + \dots + x_{n-1}A^2 + x_n A.$$

Then F is an invariant subspace of X.

A generalization of φ is the following linear map:

$$\begin{aligned} \varphi_a : \mathbb{F}^n &\longrightarrow \mathbb{F}^n \\ (x_1, \ldots, x_n) &\longrightarrow (a \cdot x_n, x_1, \ldots, x_{n-1}) \end{aligned}$$

where $a \neq 0$ and associated matrix respect to the standard basis,

$$A_a = \begin{pmatrix} 0\ 0 \ldots 0\ a \\ 1\ 0 \ldots 0\ 0 \\ 0\ 1 \ldots 0\ 0 \\ \vdots\ \vdots\ \ddots\ \vdots\ \vdots \\ 0\ 0 \ldots 1\ 0 \end{pmatrix}.$$

This linear map verifies $A_a^{-1} = A_{1/a}^t$ and $A_a^n = aI_n$. Cayley Hamilton Theorem ensures that the characteristic polynomial is

$$p(s) = \det(A - sI_n) = (-1)^n(s^n - a).$$

As in the case of the map φ, we need to compute the centralizer of the linear map A_a, in order to obtain the hyperinvariant subspaces.

Proposition 2.6. *The centralizer $\mathcal{C}(A_a)$ of A_a is the set of matrices*

$$X_a = \begin{pmatrix} x_1 & ax_2 \ldots ax_{n-1} & ax_n \\ x_n & x_1 \ \ldots ax_{n-2} & ax_{n-1} \\ x_{n-1} & x_n \ \ldots ax_{n-3} & ax_{n-2} \\ \vdots & \vdots \ \ddots \quad \vdots & \vdots \\ x_2 & x_3 \ \ldots \quad x_n & x_1 \end{pmatrix}$$

Proof. It suffices to solve the matrix equation $A_aX_a - X_aA_a = 0$.

Remark 2.3. *If $X_a \in \mathcal{C}(A_a)$ then $X_a^t \in \mathcal{C}(A_{1/a})$. For that, it suffices to observe that*

$$X_a^t = Y_{1/a} = \begin{pmatrix} y_1 & \frac{1}{a}y_n & \cdots & \frac{1}{a}y_3 & \frac{1}{a}y_2 \\ y_2 & y_1 & \cdots & \frac{1}{a}y_{n-3} & \frac{1}{a}y_{n-2} \\ y_3 & y_2 & \cdots & \frac{1}{a}y_{n-3} & \frac{1}{a}y_{n-2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ y_n & y_{n-1} & \cdots & y_2 & y_1 \end{pmatrix} \in \mathcal{C}(A_{1/a})$$

where $y_1 = x_1$ and $y_i = ax_i$ for all $i \neq 1$.

Proposition 2.7. *Let F be a hyperinvariant subspace of A_a. Then, $F^\perp$ is a hyperinvariant subspace of $A_{1/a}$.*

Proof. Given any $w \in F^\perp$, $c \in F$, $X \in \mathcal{C}(A_a)$, if $(w')^t = X^tw^t$ then, we have:

$$w'c^t = wXc^t = 0$$

and then $X^tw^t = (w')^t \in F^\perp$ and $F^\perp$ is invariant for any matrix in $\mathcal{C}(A_{1/a})$; that is to say, it is an hyperinvariant subspace for $A_{1/a}$.

Notice that if $v = (v_1, \ldots, v_n)$ is an eigenvector of A_a, then the following equalities hold:

$$\begin{aligned} av_n &= \lambda v_1 \\ v_1 &= \lambda v_2 \\ &\cdots \\ v_{n-2} &= \lambda v_{n-1} \\ v_{n-1} &= \lambda v_n \end{aligned} \tag{4}$$

In particular, we obtain that

$$v = (\lambda^{n-1}, \lambda^{n-2}, \ldots, \lambda, 1)$$

and we have the following Proposition:

Proposition 2.8. *Given any $\lambda \in GF(q)^*$ such that $\lambda^n = a$, then $[v]$ with $v = (\lambda^{n-1}, \lambda^{n-2}, \ldots, \lambda, 1)$ is an hyperinvariant subspace.*

Proposition 2.5 can be generalized to the case of A_a maps.

Proposition 2.9. *Let F be an invariant subspace of A_a. Then it is hyperinvariant.*

Proof. It suffices to observe that, for all $X_a \in \mathcal{C}(A_a)$,

$$X_a = x_1I + x_2A_a^{n-1} + \ldots + x_{n-1}A_a^2 + x_nA_a.$$

Then F is an invariant subspace of X_a.

Example 2.2. *Over $\mathbb{F} = GF(5)$ we consider*

$$A_a = \begin{pmatrix} 0\ 0\ 2 \\ 1\ 0\ 0 \\ 0\ 1\ 0 \end{pmatrix}$$

$F = [(1, 2, 4)]$ is invariant

$$\begin{pmatrix} 0\ 0\ 2 \\ 1\ 0\ 0 \\ 0\ 1\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} = 3 \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}$$

and also it is hyperinvariant

$$\begin{pmatrix} x_1 & 2x_2 & 2x_3 \\ x_3 & x_1 & 2x_2 \\ x_2 & x_3 & x_1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix} = (x_1 + 4x_2 + 3x_3) \begin{pmatrix} 1 \\ 2 \\ 4 \end{pmatrix}.$$

Notice that in fact we have solved the following slightly more general case

$$\begin{aligned}\varphi_{ab} : \mathbb{F}^n &\longrightarrow \mathbb{F}^n\\ (x_1, \dots, x_n) &\longrightarrow (a \cdot x_n, b \cdot x_1, \dots, b \cdot x_{n-1})\end{aligned}$$

with associated matrix with respect to the standard basis,

$$A_{ab} = \begin{pmatrix} 0\,0 \dots 0\; a \\ b\; 0 \dots 0\; 0 \\ 0\; b \dots 0\; 0 \\ \vdots\; \vdots\; \ddots\; \vdots\; \vdots \\ 0\; 0 \dots b\; 0 \end{pmatrix}.$$

for a, b such that $ab \neq 0$ because of

$$A_{ab}X - XA_{ab} = D(A_{a/b}X - XA_{a/b})$$

with $D = \text{diag}\,(b)$.

Finally we show the two parameter case. Given two different non-zero elements α, β in $\mathbb{F}$, we are interested in the following linear map

$$\begin{aligned}\varphi_{\alpha,\beta} : \mathbb{F}^n &\longrightarrow \mathbb{F}^n\\ (x_1, \dots, x_n) &\longrightarrow (\beta \cdot x_n, x_1, \alpha \cdot x_2 \dots, \alpha \cdot x_{n-1})\end{aligned}$$

with associated matrix with respect to the standard basis,

$$A_{\alpha,\beta} = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & \beta \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \alpha & 0 & \dots & 0 & 0 \\ 0 & 0 & \alpha & \dots & 0 & 0 \\ \vdots & & & \ddots & & \\ 0 & 0 & 0 & \dots & \alpha & 0 \end{pmatrix}$$

The characteristic polynomial of $A_{\alpha,\beta}$ is $p_{\alpha,\beta}(s) = (-1)^n(s^n - \alpha^{n-2}\beta)$,

Proposition 2.10. *The centralizer $\mathcal{C}(A_{\alpha,\beta})$ of $A_{\alpha,\beta}$ is the set of matrices $X_{\alpha,\beta}$ with:*

$$X_{\alpha,\beta} = \begin{pmatrix} x_n & \beta x_1 & \frac{\beta}{\alpha}x_2 & \frac{\beta}{\alpha}x_3 & \dots & \frac{\beta}{\alpha}x_{n-2} & \frac{\beta}{\alpha}x_{n-1} \\ \frac{1}{\alpha}x_{n-1} & x_n & \frac{\beta}{\alpha}x_1 & \frac{\beta}{\alpha^2}x_2 & \dots & \frac{\beta}{\alpha^2}x_{n-3} & \frac{\beta}{\alpha^2}x_{n-2} \\ \vdots & & \ddots & \ddots & & & \\ \vdots & & & \ddots & \ddots & & \\ \frac{1}{\alpha}x_3 & x_4 & x_5 & x_6 & \dots & \frac{\beta}{\alpha}x_1 & \frac{\beta}{\alpha^2}x_2 \\ \frac{1}{\alpha}x_2 & x_3 & x_4 & x_5 & \dots & x_n & \frac{\beta}{\alpha}x_1 \\ x_1 & x_2 & x_3 & x_4 & \dots & x_{n-1} & x_n \end{pmatrix}$$

The proof is analogous to those of Propositions 2.1 and 2.6.

Notice that if $v = (v_1, \dots, v_n)$ is an eigenvector of $A_{\alpha,\beta}$, then:

$$\begin{aligned}\beta v_n &= \lambda v_1\\ v_1 &= \lambda v_2\\ &\dots\\ \alpha v_{n-2} &= \lambda v_{n-1}\\ \alpha v_{n-1} &= \lambda v_n\end{aligned} \tag{5}$$

In particular, we obtain that

$$v = (\lambda^{n-1}\alpha^{-(n-2)}, \lambda^{n-2}\alpha^{-(n-2)}, \dots, \lambda\alpha^{-1}, 1)$$

and we have the following Proposition:

Proposition 2.11. *Given any $\lambda \in GF(q)^*$ such that $\lambda^n = \beta\alpha^{n-2}$, then $v]$ with $v = (\lambda^{n-1}\alpha^{-(n-2)}, \lambda^{n-2}\alpha^{-(n-2)}, \dots, \lambda\alpha^{-1}, 1)$ is an hyperinvariant subspace.*

Proposition 2.12. *Let F be an invariant subspace of $A_{\alpha,\beta}$. Then it is hyperinvariant.*

Proof. It suffices to observe that, for all $X_{\alpha,\beta} \in \mathcal{C}(A_{\alpha,\beta})$ then

$$\begin{aligned}&X_{\alpha,\beta} =\\ &x_nI + \frac{x_1}{\alpha^{n-2}}A_{\alpha,\beta}^{n-1} + \frac{x_2}{\alpha^{n-3}}A_{\alpha,\beta}^{n-3} + \dots +\\ &\qquad \frac{x_{n-2}}{\alpha^2}A_{\alpha,\beta}^2 + \frac{x_{n-1}}{\alpha}A_{\alpha,\beta}.\end{aligned}$$

3 Linear cyclic codes

Throughout this section, $\mathbb{F}$ denotes a fixed finite field and n a positive integer such that the characteristic of $\mathbb{F}$ does not divide the length of the code n. This condition is the usual assumption from the theory of cyclic block codes in order to guarantee that the polynomial $s^n - 1$ factorize into different prime polynomials over $\mathbb{F}$.

Definition 3.1. *A code C with length n over the field $\mathbb{F}$ is called cyclic, if whenever $c = (a_1, \dots, a_n)$ is in C, its cycle shift $sc = (a_n, a_1, \dots, a_{n-1})$ is also in C.*

Example 3.1. *The linear code $C = \{000, 110,\ 011, 101\}$ over $GF(2)$ is cyclic. To prove that, we compute the shift sc for all $c \in C$: $s(000) = 000$, $s(110) = 011$, $s(011) = 101$, and $s(101) = 110$.*

It is easy to prove the following statement from the definitions.

Let P_3 be a full cycle permutation matrix obtained from the identity matrix I_3 by moving its first column to the last column (observe that P_3 corresponds to the matrix A of Equation (2) for $n = 3$). The shift sc can be expressed as

$$\begin{pmatrix} 0\,0\,1 \\ 1\,0\,0 \\ 0\,1\,0 \end{pmatrix} \begin{pmatrix} 0\,1\,0\,1 \\ 0\,1\,1\,0 \\ 0\,0\,1\,1 \end{pmatrix} = \begin{pmatrix} 0\,0\,1\,1 \\ 0\,1\,0\,1 \\ 0\,1\,1\,0 \end{pmatrix}$$

In general the shift sc can be expressed as $P_n c^t$ where P_n be a full cycle permutation matrix obtained from the identity matrix I_n by moving its first column to the last column.

Taking into account that P_n is a linear transformation of $\mathbb{F}^n$ (the map φ defined in Equation (1)), we can construct a cyclic code, as follows: take a word c, and construct the set S consisting of c and its successive images by this linear map

$$S = \{c^t, P_n c^t, \dots, P_n^{n-1} c^t\}$$

and define the linear subspace C as the linear space generated by S; that is to say, $C = [S]$. Then C is defined as the smallest linear cyclic code containing c.

The two Propositions below are proved in [Radkova, Van-Zanten, 2009] and [Radkova, Bojilov, Van-Zanten, 2007].

Proposition 3.1. *A linear code C with length n over the field $\mathbb{F}$ is cyclic if, and only if, C is a P_n-invariant subspace of $\mathbb{F}^n$.*

Proposition 3.2. *Let C be a cyclic code, and $p(s) = (-1)^n p_1(s) \cdot \ldots \cdot p_r(s)$ the decomposition of $p(s)$ in irreducible factors. Then $C = \operatorname{Ker} p_{i_1}(A) \oplus \ldots \oplus \operatorname{Ker} p_{i_s}(A)$ for some minimal φ-invariant subspaces $\operatorname{Ker} p_{i_j}(A)$ of $\mathbb{F}^n$.*

After Proposition 2.5 we deduce the following result.

Proposition 3.3. *A linear code C with length n over the field $\mathbb{F}$ is cyclic if, and only if, C is a P_n-hyperinvariant subspace of F^n.*

Example 3.2. *Consider the matrix A of φ for $n = 7$ and $q = 2$. Then we have $p(s) = s^7 + 1$. Factorizing $p(s)$ into irreducible factors over $GF(2)$ we have $p(s) = p_1(s)p_2(s)p_3(s) = (s+1)(s^3+s+1)(s^3+s^2+1)$. The factors $p_i(s)$ define minimal P_n-invariant subspaces $F_i = \operatorname{Ker} p_i(A)$, for $i = 1, 2, 3$.*

We define a cyclic linear code C by

$$C = F_1 \oplus F_2 = \operatorname{Ker}(p_1(A)) \oplus \operatorname{Ker}(p_2(A))$$

$p_1(s) \cdot p_2(s) = s^4 + s^3 + s^2 + 1$ *and* $A^4 + A^3 + A^2 + I$ *is the following matrix*

$$\begin{pmatrix} 1\,0\,0\,1\,1\,1\,0 \\ 0\,1\,0\,0\,1\,1\,1 \\ 1\,0\,1\,0\,0\,1\,1 \\ 1\,1\,0\,1\,0\,0\,1 \\ 1\,1\,1\,0\,1\,0\,0 \\ 0\,1\,1\,1\,0\,1\,0 \\ 0\,0\,1\,1\,1\,0\,1 \end{pmatrix}$$

$$\operatorname{Ker}(A^4 + A^3 + A^2 + I) = \\ [(1,0,1,1,0,0,0),(1,1,1,0,1,0,0),(1,1,0,0,0,1,0), \\ (0,1,1,0,0,0,1)].$$

4 Constacyclic codes

As a first generalization of cyclic codes we have the constacyclic codes which were introduced in [Berlekamp, 1968].

Definition 4.1. *Let a be a nonzero element of $\mathbb{F}$. A code C with length n over the field $\mathbb{F}$ is called constacyclic with respect to a if whenever $c = (a_1, \dots, a_n)$ is in C, so is its cycle constashift $sc = (a \cdot a_n, a_1, \dots, a_{n-1})$.*

Obviously, when $a = 1$ the constacyclic code is cyclic.

The constashift sc can be expressed as $P_{a_n} c^t$ where P_{a_n} is a generalized full cycle permutation matrix obtained from the identity matrix I_n by moving its first column multiplied by a to the last column.

$$P_{a_n} = \begin{pmatrix} 0 & 0 & \dots & 0 & a \\ 1 & 0 & & 0 & 0 \\ \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

According to [Radkova, Van-Zanten, 2009], we have the following Propositions.

Proposition 4.1. *A linear code C with length n over the field $\mathbb{F}$ is constacyclic if, and only if, C is an P_{a_n}-invariant subspace of $\mathbb{F}^n$.*

Suppose now that $(n, q) = 1$ and $p_a(s) = (-1)^n(s^n - a)$ has no multiple roots and splits into distinct irreducible monic factors.

Proposition 4.2. *Let C be a constacyclic code, and $p_a(s) = (-1)^n p_{a_1}(s) \cdot \ldots \cdot p_{a_r}(s)$ the decomposition of $p_a(s)$ in irreducible factors. Then $C = \operatorname{Ker} p_{a_{i_1}}(A) \oplus \ldots \oplus \operatorname{Ker} p_{a_{i_s}}(A)$ for some minimal φ_a-invariant subspaces $\operatorname{Ker} p_{a_{i_j}}(A)$ of $\mathbb{F}^n$.*

After Proposition 2.9 we deduce the following result.

Proposition 4.3. *A linear code C with length n over the field $\mathbb{F}$ is constacyclic if and only if C is an P_{a_n}-hyperinvariant subspace of $\mathbb{F}^n$.*

Example 4.1. *Consider the matrix A_a of P_{a_n} for $n = 8$, $q = 5$ and $a = 4$. Then we have $p(s) = s^8 - 4$. Factorizing $p(s)$ into irreducible factors over $GF(5)$ we have $p(s) = p_1(s)p_2(s) = (s^4 - 2)(s^4 + 2)$. The factors $p_i(s)$ define minimal P_{a_n}-invariant subspaces $F_i = \operatorname{Ker} p_i(A_a)$, for $i = 1, 2$.*

We define a constacyclic linear code C_a by

$$C_a = F_1 = \operatorname{Ker}(p_1(A))$$

$p_1(s) = s^4 - 2$ and $A^4 - 2I$ is the following matrix

$$\begin{pmatrix} 3&0&0&0&4&0&0&0\\ 0&3&0&0&0&4&0&0\\ 0&0&3&0&0&0&4&0\\ 0&0&0&3&0&0&0&4\\ 1&0&0&0&3&0&0&0\\ 0&1&0&0&0&3&0&0\\ 0&0&1&0&0&0&3&0\\ 0&0&0&1&0&0&0&3 \end{pmatrix}$$

$$\begin{array}{l}\mathrm{Ker}\,(A^4 - 2I) = \\ [(2,0,0,0,1,0,0,0),(0,2,0,0,0,1,0,0), \\ \quad (0,0,2,0,0,0,1,0),(0,0,0,2,0,0,0,1)]\,. \end{array}$$

5 Two-parameter cyclic codes

In this section, we will to generalize the concept of constacyclic code to two parameter cyclic code as follows.

Definition 5.1. *Let α, β be two nonzero elements of $\mathbb{F}$. A code C with length n over the field $\mathbb{F}$ is called two-parameter cyclic with respect to α and β if whenever $c = (a_1, \ldots, a_n)$ is in C, so is its cycle two parameter shift $sc = (\beta \cdot a_n, a_1, \alpha \cdot a_2 \ldots, \alpha \cdot a_{n-1})$.*

Obviously, when $\alpha = 1$ the two-parameter cyclic code is constacyclic and when $\alpha = \beta = 1$ it is cyclic.

The two-parameter shift sc can be expressed as $P_{\alpha,\beta_n} c^t$ where P_{α,β_n} is a generalized full cycle permutation matrix obtained from the identity matrix I_n multiplying by α the third to n column and by moving its first column multiplied by β to the last column.

$$P_{\alpha,\beta_n} = \begin{pmatrix} 0 & 0 & \ldots & 0 & \beta \\ 1 & 0 & & 0 & 0 \\ 0 & \alpha & & 0 & 0 \\ \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & \ldots & \alpha & 0 \end{pmatrix}$$

As immediate consequence of definition we have the following Proposition.

Proposition 5.1. *A linear code C with length n over the field $\mathbb{F}$ is two-parameter cyclic if, and only if, C is an P_{α,β_n}-invariant subspace of $\mathbb{F}^n$.*

After Proposition 2.12 we have the following result.

Proposition 5.2. *A linear code C with length n over the field $\mathbb{F}$ is two-parameter cyclic if, and only if, C is a P_{α,β_n}-hyperinvariant subspace of $\mathbb{F}^n$.*

Suppose now that $(n, q) = 1$ and $p_{\alpha,\beta}(s)$ has no multiple roots and splits into distinct irreducible monic factors.

Proposition 5.3. *Let C be a two parameter cyclic code, and $p_{\alpha,\beta}(s) = (-1)^n p_{\alpha,\beta_1}(s) \cdot \ldots \cdot p_{\alpha,\beta_r}(s)$ the decomposition of $p_{\alpha,\beta}(s)$ in irreducible factors. Then $C = \mathrm{Ker}\, p_{\alpha,\beta_{i_1}}(A_{\alpha,\beta}) \oplus \ldots \oplus \mathrm{Ker}\, p_{\alpha,\beta_{i_s}}(A_{\alpha,\beta})$ for some minimal P_{α,β_n}-invariant subspaces $\mathrm{Ker}\, p_{\alpha,\beta_{i_j}}(A_{\alpha,\beta})$ of $\mathbb{F}^n$.*

Proof. First of all, it is easy to see that $\mathrm{Ker}\, p_{\alpha,\beta_i}(A_{\alpha,\beta})$ for $i = 1, \ldots, r$ are P_{α,β_n}-invariant: let $v \in \mathrm{Ker}\, p_{\alpha,\beta_i}(A_{\alpha,\beta})$ then $P_{\alpha\beta_n} v = p_{\alpha,\beta_1}(A_{\alpha\beta}) \cdot \ldots \cdot p_{\alpha,\beta_r}(A_{\alpha,\beta})v = 0$.

The subspaces $\mathrm{Ker}\, p_{\alpha,\beta_{i_j}}(A_{\alpha,\beta})$ are minimal because the polynomials $p_{\alpha,\beta_i}(s)$ are irreducible.

Now, we define $\widehat{p}_i(s) = p_{\alpha,\beta}(s)/p_{\alpha,\beta_i}(s)$. Taking into account $(\widehat{p}_1(s), \ldots, \widehat{p}_r(s)) = 1$, there exist polynomials $q_1(s), \ldots, q_r(s)$ such that $q_1(s)\widehat{p}_1(s) + \ldots + q_r(s)\widehat{p}_r(s) = 1$.

Let $c \in C$, then $c = q_1(A_{\alpha,\beta})\widehat{p}_1(A_{\alpha,\beta})c + \ldots + q_r(A_{\alpha,\beta})\widehat{p}_r(A_{\alpha,\beta})c$. Calling $c_i = q_i(A_{\alpha,\beta})\widehat{p}_i(A_{\alpha,\beta})c$ and taking into account that C is $P_{\alpha,\beta}$-invariant, and that $c_i \in \mathrm{Ker}\, p_{\alpha,\beta_i}(A_{\alpha,\beta})$ we have that $c_i \in C \cap \mathrm{Ker}\, p_{\alpha,\beta_i}(A_{\alpha,\beta})$.

Example 5.1. *Consider the matrix $A_{\alpha,\beta}$ of P_{α,β_n} for $n = 8$, $q = 5$, $\alpha = 2$ and $\beta = 4$. Then we have $p(s) = s^8 - 1$. Factorizing $p(s)$ into irreducible factors over $GF(5)$ we have $p(s) = p_1(s)p_2(s)p_3(s)p_4(s)p_5(s)p_6(s) = (s+1)(s+2)(s+3)(s+4)(s^2+2)(s^2+3)$. The factors $p_i(s)$ define minimal P_{α,β_n}-invariant subspaces $F_i = \mathrm{Ker}\, p_i(A_{\alpha,\beta})$, for $i = 1, 2, 3, 4, 5, 6$.*

We define a two-parameter cyclic linear code $C_{\alpha\beta}$ by

$$C_{\alpha,\beta} = F_1 \oplus F_5 = \mathrm{Ker}\,(p_1(A_{\alpha,\beta})) \oplus \mathrm{Ker}\,(p_5(A_{\alpha,\beta}))$$

$p_1(s) \cdot p_5(s) = s^3 + s^2 + 2s + 2$ and $A^3_{\alpha,\beta} + A^2_{\alpha,\beta} + 2A_{\alpha,\beta} + 2I$ is the following matrix

$$\begin{pmatrix} 2&0&0&0&0&1&3&3\\ 2&2&0&0&0&0&3&4\\ 2&4&2&0&0&0&0&3\\ 4&4&4&2&0&0&0&0\\ 0&3&4&4&2&0&0&0\\ 0&0&3&4&4&2&0&0\\ 0&0&0&3&4&4&2&0\\ 0&0&0&0&3&4&4&2 \end{pmatrix}$$

$$\begin{array}{l}\mathrm{Ker}\,(A^3_{\alpha,\beta} + A^2_{\alpha,\beta} + 2A_{\alpha,\beta} + 2I) = \\ [(1,4,2,1,3,4,2,1),(1,0,4,0,2,0,1,0), \\ \quad (0,3,0,4,0,2,0,1)]\,. \end{array}$$

6 Cyclic codes as convolutional codes

The cyclic block codes can be represented by means of polynomials in the following way

$$\begin{array}{rl} p : \mathbb{F}^n & \longrightarrow \mathbb{F}[s]/(s^n - 1) \\ c = (a_0, \ldots, a_{n-1}) & \longrightarrow p(c) = \sum_{i=0}^{n-1} a_i s^i \end{array}$$

The map p translates the cyclic shift into multiplication by s. As a consequence, a cyclic block code C can be represented as an ideal $p(C)$ in $\mathbb{F}[s]/(s^n-1)$ and vice versa.

In fact, we have the following Proposition.

Proposition 6.1. *A linear code C is cyclic if and only if $p(C)$ is an ideal of $\mathbb{F}[s]/(s^n-1)$.*

Proposition 6.2. *Let C be a cyclic code, then there exists a monic polynomial $g(s)$ of minimal degree r such that $p(C)=\langle g(s)\rangle$, and dimension of $p(C)$ is $n-r$.*

$$p(C)=\langle p(s)g(s)\mid \textit{degree}\, p(s)<n-r\rangle$$

This Proposition allows to view the cyclic code as convolutional code defining the encoder by

$$G(s)=\begin{pmatrix} g(s)\\ sg(s)\\ \vdots\\ s^{n-r-1}g(s)\end{pmatrix}.$$

Example 6.1. *Let* $\{(000000),\ (111000),\ (000111),\ (111111)\}$ *be some codewords of a cyclic code.*

Considering their images,

$p(C)=\{1+s+s^2, s^3+s^4+s^5, 1+s+s^2+s^3+s^4+s^5\}\subset[1+s+s^2, s^3+s^4+s^5, 1+s+s^2+s^3+s^4+s^5]$ *in* $\mathbb{F}[s]/(s^6-1)$.

Observe that $s^6-1=(s^2+s+1)(s^4+s^3+s+1)$ *and* $s^3+s^4+s^5=s^3(s^2+s+1)$, $1+s+s^2+s^3+s^4+s^5=(1+s^3)(s^2+s+1)$, *then* $1+s+s^2$ *can be the generator of the code.*

Then the ideal $p(C)$ *is generated by* $\langle g(s)\rangle=\langle 1+s+s^2\rangle$, *the dimension is* $n-\textit{degre}\,g(s)=6-2=4$ *and* C *is constituted by the multiples of* $g(s)$, $C=\{1+s+s^2, s+s^2+s^3, s^2+s^3+s^4, s^3+s^4+s^5\}$.

The corresponding $(4,1,5)$ *convolutional code is the rational matrix associated* $G(s)$ *defined as follows:*

$$\begin{pmatrix}1+s+s^2\\ s+s^2+s^3\\ s^2+s^3+s^4\\ s^3+s^4+s^5\end{pmatrix}=\begin{pmatrix}\frac{1+s+s^2}{s^3+s^4+s^5}\\ \\ \frac{s+s^2+s^3}{s^3+s^4+s^5}\\ \\ \frac{s^2+s^3+s^4}{s^3+s^4+s^5}\\ \\ 1\end{pmatrix}(s^3+s^4+s^5)=$$

$$G(s)(s^3+s^4+s^5).$$

A realization of this code is (A,B,C,D) *where* $A=\begin{pmatrix}-1&-1&0&0&0\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\end{pmatrix}$, $B=\begin{pmatrix}1\\0\\0\\0\\0\end{pmatrix}$, $C=\begin{pmatrix}0&0&1&1&1\\ 0&1&1&1&0\\ 1&1&1&0&0\end{pmatrix}$, $D=0_{3\times 1}$.

It is easy to verify that $C(sI-A)^{-1}B+D=\begin{pmatrix}\frac{1+s+s^2}{s^3+s^4+s^5}\\ \\ \frac{s+s^2+s^3}{s^3+s^4+s^5}\\ \\ \frac{s^2+s^3+s^4}{s^3+s^4+s^5}\\ \\ 1\end{pmatrix}.$

Notice that this system in not minimal, controllable but not observable (see in [Garcia-Planas, Souidi, Um, 2013]).

Simplifying the fractions in $G(s)$ *we observe that the matrix* $G(s)$ *is equivalent to* $\widetilde{G}(s)=\begin{pmatrix}\frac{1}{s^3}\\ \\ \frac{s}{s^3}\\ \\ \frac{s^2}{s^3}\\ \\ 1\end{pmatrix}.$

The realization of this rational matrix is given by $(\widetilde{A},\widetilde{B},\widetilde{C},\widetilde{D})$ *where* $\widetilde{A}=\begin{pmatrix}0&0&0\\ 1&0&0\\ 0&1&0\end{pmatrix}$, $\widetilde{B}=\begin{pmatrix}1\\0\\0\end{pmatrix}$, $\widetilde{C}=\begin{pmatrix}0&0&1\\ 0&1&0\\ 1&0&0\end{pmatrix}$ *and* $D=0_{3\times 1}$.

It is easy to show that $C(sI-A)^{-1}B+D=\widetilde{G}(s)$.

This realization is minimal, controllable and observable, (see more in [Garcia-Planas, Souidi, Um, 2013]).

In general, given $G(s)$ associated to a cyclic code, we observe that it is equivalent to the matrix

$$\widetilde{G}(s)=\begin{pmatrix}\dfrac{1}{s^{n-r-1}}\\ \dfrac{s}{s^{n-r-1}}\\ \vdots\\ \dfrac{s^{n-r-2}}{s^{n-r-1}}\\ 1\end{pmatrix}$$

A realization of this convolutional code is

$(\widetilde{A},\widetilde{B},\widetilde{C},\widetilde{D})$ where

$$\begin{aligned}
A &= \begin{pmatrix} 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & \dots & 0 & 0 \\ & \ddots & & & \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix} \in M_{n-r-1}(\mathbb{F}), \\
B &= \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in M_{(n-r-1)\times 1}(\mathbb{F}), \\
C &= \begin{pmatrix} 0 & \dots & 0 & 1 \\ 0 & \dots & 1 & 0 \\ & \iddots & & \\ 1 & \dots & 0 & 0 \end{pmatrix} \in M_{n-r-1}(\mathbb{F}) \\
D &= 0_{(n-r-1)\times 1}.
\end{aligned} \tag{6}$$

And we have the following Proposition.

Proposition 6.3. *A sufficient condition for the linear system (A,B,C,D) be the realization of a linear cyclic code is that it is equivalent to the system $(\widetilde{A},\widetilde{B},\widetilde{C},\widetilde{D})$ considered in* (6)*, under the equivalence relation $(\widetilde{A},\widetilde{B},\widetilde{C},\widetilde{D}) = (P^{-1}AP, P^{-1}B, CP, D)$.*

Remark 6.1. *The equivalence relation considered preserve the transfer matrix of the system:*

$$\begin{aligned}
&\widetilde{C}(sI-\widetilde{A})^{-1}\widetilde{B}+\widetilde{D} = \\
&CP(sI-P^{-1}AP)^{-1}P^{-1}B+D = \\
&CPP^{-1}(sI-A)^{-1}PP^{-1}B+D = \\
&C(sI-A)^{-1}B+D.
\end{aligned}$$

References

Astuti P., Wimmer, H.K. (2011) Characteristic and hyperinvariant subspaces over the field GF(2), *Linear Algebra Appl*, doi:10.1016/j.laa.2011.03.047. **2**, Dallas, TX, pp. 974-978.

Berlekamp E.R., (1968). “Algebraic Coding Theory”, Mc Graw-Hill Book Company, New York.

Garcia-Planas M.I., Soudi El M., Um L.E. (2013). *Convolutional codes under control theory point of view. Analysis of output-observability*. Recent Advances in Circuits, Communications & Signal Processing, pp. 131–137.

Gluesing-Luerssen H., Schmale W. (2004) On Cyclic Convolutional Codes, Acta Applicandae Mathematicae **82**, pp. 183–237.

MacWilliams F.G., Sloane N. J. A. (1977). “The Theory of Error Correcting Codes”. North-Holland Publ. Company, Amsterdam.

Radkova D., Bojilov A., Van Zanten A.J., (2007). *Cyclic codes and quasi-twisted codes: an algebraic approach*, Report MICC 07-08, Universiteit Maastricht.

Radkova D., Van Zanten D.J. (2009) Constacyclic codes as invariant subspaces, Linear Algebra and its Applications **430**, pp. 855–864.