CYBERNETICS AND PHYSICS, VOL. 2, NO. 2, 2013 , 90–96

TWO PARAMETRIC QUASI-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. d'Àlgebra i Geometria
Universitat de Barcelona
Spain
maria.eulalia.montoro@upc.edu

Abstract
It is known the relationship between cyclic codes and invariant subspaces. In this work we present a generalization considering "generalized" cyclic codes and hyperinvariant subspaces.

Key words
Cyclic codes, two-parametric quasi cyclic codes, hyperinvariant subspaces.

1 Introduction

Let φ be an endomorphism of a vector space V over a field $\mathbb{F}$.

Recall that 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 establish the relationship between the set of some "generalized cyclic codes" and hyperinvariant linear subspaces of $\mathbb{F}^n$.

Despite of the fact that Commutative Algebra is the tool mostly used to study linear cyclic codes (see [MacWilliams and Sloane, 1977], for example), since linear codes have a structure of linear subspaces of $\mathbb{F}^n$, they can also be studied using Linear Algebra as [Garcia-Planas, Souidi and Um, 2012; Garcia-Planas, Souidi and Um, 2013].

2 Preliminaries

2.1 Hyperinvariant Subspaces of Cyclic Permutation Maps

Let p be a prime number, $q = p^k$ for some $k \geq 1$ and $\mathbb{F} = GF(q)$. Let $\mathbb{F}^n$ be the n-dimensional vector space over the field $\mathbb{F}$.

We consider the following linear map

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

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 (in the sense $A^t = A^{-1}$) and verifies $A^n = I_n$. Cayley Hamilton Theorem ensures that its characteristic polynomial is

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

To study hyperinvariant subspaces (those which are invariant for all linear maps commmuting with φ) we need to compute the centralizer of 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. *Two matrices belonging to a given centralizer do not necessarily commute. But in our case, given any circulant matrix X commuting with A, its centralizer is $\mathcal{C}(X) = \mathcal{C}(A)$.*

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

Lemma 2.1.

$$X \in \mathcal{C}(A)$$

if, and only if,

$$X^t \in \mathcal{C}(A)$$

.

Proof. All circulant matrices satisfy $XX^t = X^tX$ (they are normal matrices) and the Lemma follows.

Proposition 2.2. *If F is φ-hyperinvariant subspace, $F^\perp$ is also an hyperinvariant subspace.*

Proof. Given any $w \in F^\perp$, $v \in F$, $X \in \mathcal{C}(A)$, we wish to prove that $Xw^t \in F^\perp$. Since

$$(Xw^t)^t v^t = wX^t v^t$$

and taking into account Lemma 2.1 we have that $X^t v^t \in F$ and therefore:

$$wX^t v^t = 0$$

We conclude that $Xw^t \in F^\perp$ 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 any eigenvector of A has the form.

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

We can derive the following Proposition.

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

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

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 $\mathbb{F} = GF(7)$ and $n = 6$. The characteristic polynomial of A has, in this particular set-up, six different roots. In particular, the eigenvalues of A are $\lambda_1 = 1$, $\lambda_2 = 2$, $\lambda_3 = 3$, $\lambda_4 = 4$, $\lambda_5 = 5$, $\lambda_6 = 6$.*

In general, we have the following result.

Proposition 2.4. *Let v be 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 a simple root of the characteristic polynomial of a, we have that $Xv = \lambda v$, and the proof is completed.

We can compute the value of the eigenvalue associated to v as follows.

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

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

Then λ is equal to the i-th coordinate of Xv, $x_{n-i+2}v_1 + \dots + x_{n-i+1}v_n$.

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

Proposition 2.5. *Let F be a φ-invariant subspace. Then F it is hyperinvariant.*

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

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

Then F is an invariant subspace of X.

2.2 Linear Cyclic Codes

Let us assume that characteristic of $\mathbb{F}$ does not divide the length of the code n. This assumption is an usual one in 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 2.2. *A code C of 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 2.2. *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 is 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 as defined in Equation (1)), we can construct a cyclic code, as follows. Take a word c, and consider the set S consisting of c and its successive images by P_n:

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

The linear subspace C, defined as the linear space spanned by S, $C = [S]$, is the smallest linear cyclic code containing c.

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

Proposition 2.6. *A linear code C of length n over the field $\mathbb{F}$ is cyclic if, and only if, C is an A-invariant subspace of $\mathbb{F}^n$.*

Proposition 2.7. *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 prime 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 2.8. *A linear code C with length n over the field $\mathbb{F}$ is cyclic if, and only if, C is an A-hyperinvariant subspace of F^n.*

Example 2.3. *Consider the matrix A of φ for $n = 7$ and $q = 2$. Then we have $p(s) = s^7 + 1$. Factorizing $p(s)$ into prime factors over $GF(2)$ we have that $p(s) = p_1(s)p_2(s)p_3(s) = (s+1)(s^3+s+1)(s^3+s^2+1)$. 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

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

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

3 Generalized Case

If $q > 2$, we can generalize the above case as follows.

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

with associated matrix with respect to the standard basis,

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

for a, b, c such that $abc \neq 0$.

The characteristic polynomial of $A_{a,b,c}$ is $p_{a,b,c}(s) = (-1)^n (s^n - c^{n-2}ab)$,

Proposition 3.1. *The centralizer $\mathcal{C}(A_{a,b,c})$ of $A_{a,b,c}$ is* *the set of matrices $X_{a,b,c}$ with:*

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

Proof. It suffices to solve the matrix equation $A_{a,b,c}X_{a,b,c} - X_{a,b,c}A_{a,b,c} = 0$.

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

$$\begin{aligned} av_n &= \lambda v_1 \\ bv_1 &= \lambda v_2 \\ cv_2 &= \lambda v_3 \dots \\ cv_{n-2} &= \lambda v_{n-1} \\ cv_{n-1} &= \lambda v_n \end{aligned} \tag{4}$$

In particular, we obtain that

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

and we have the following Proposition.

Proposition 3.2. *Let $\lambda \in GF(q)^*$ be an element such that $\lambda^n = abc^{n-2}$. Then $[v] = [(\lambda^{n-1}b^{-1}c^{-(n-2)}, \lambda^{n-2}c^{-(n-2)}, \dots, \lambda c^{-1}, 1)]$ is an hyperinvariant subspace.*

Proof.

$$A_{a,b,c}v = \lambda v$$

and given any $X_{a,b,c} \in \mathcal{C}(A_{a,b,c})$, then

$$\begin{aligned} &X_{a,b,c}v = \\ &(x_1 I + \frac{x_2}{c}A_{a,b,c} + \frac{x_3}{c^2}A^2_{a,b,c} + \dots + \\ &+\frac{x_{n-1}}{c^{n-2}}A^{n-2}_{a,b,c} + \frac{x_n}{bc^{n-2}}A^{n-1}_{a,b,c})v = \\ &x_1 v + \frac{x_2}{c}\lambda v + \frac{x_3}{c^2}\lambda^2 v + \dots + \\ &+\frac{x_{n-1}}{c^{n-2}}\lambda^{n-2}v + \frac{x_n}{bc^{n-2}}\lambda^{n-1}v = \\ &\alpha v \end{aligned}$$

with $\alpha = x_1 + \frac{x_2}{c}\lambda + \frac{x_3}{c^2}\lambda^2 + \dots + +\frac{x_{n-1}}{c^{n-2}}\lambda^{n-2} + \frac{x_n}{bc^{n-2}}\lambda^{n-1} \in \mathbb{F}$.

Proposition 3.3. *Let F be an invariant subspace of $A_{a,b,c}$. Then F is hyperinvariant.*

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

$$\begin{aligned} &X_{a,b,c} = \\ &x_1 I + \frac{x_2}{c}A_{a,b,c} + \frac{x_3}{c^2}A^2_{a,b,c} + \dots + \\ &\qquad \frac{x_{n-1}}{c^{n-2}}A^{n-2}_{a,b,c} + \frac{x_n}{bc^{n-2}}A^{n-1}_{a,b,c}. \end{aligned}$$

Therefore, we have that in this case the lattices of invariant and hyperinvariant subspaces are equal,i.e.:

$$Hinv(A_{a,b,c}) = Inv(A_{a,b,c})$$

3.1 Particular Case $b = 1$

Notice that it suffices to solve the case $b = 1$ because:

$$A_{a,b,c}X - XA_{a,b,c} = D(A_{a/b,1,c/b}X - XA_{a/b,1,c/b})$$

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

So, we write the results in this simpler case.

Given $a, c \neq 0$, we consider the following linear map:

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

with associated matrix with respect to the standard basis,

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

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

Proposition 3.4. *The centralizer $\mathcal{C}(A_{a,c})$ of $A_{a,c}$ is the set of matrices $X_{a,c}$ with:*

$$X_{a,c} = \begin{pmatrix} x_n & ax_1 & \frac{a}{c}x_2 & \frac{a}{c}x_3 & \dots & \frac{a}{c}x_{n-2} & \frac{a}{c}x_{n-1} \\ \frac{1}{c}x_{n-1} & x_n & \frac{a}{c}x_1 & \frac{a}{c^2}x_2 & \dots & \frac{a}{c^2}x_{n-3} & \frac{a}{c^2}x_{n-2} \\ \vdots & & \ddots & \ddots & & & \\ \vdots & & & \ddots & \ddots & & \\ \frac{1}{c}x_3 & x_4 & x_5 & x_6 & \dots & \frac{a}{c}x_1 & \frac{a}{c^2}x_2 \\ \frac{1}{c}x_2 & x_3 & x_4 & x_5 & \dots & x_n & \frac{a}{c}x_1 \\ x_1 & x_2 & x_3 & x_4 & \dots & x_{n-1} & x_n \end{pmatrix}$$

Proof. It follows from Proposition 3.1, when $b = 1$.

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

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

In particular, we obtain that

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

and we have the following Proposition.

Proposition 3.5. *Given any $\lambda \in GF(q)^*$ such that $\lambda^n = ac^{n-2}$, then $v = (\lambda^{n-1}c^{-(n-2)}, \lambda^{n-2}c^{-(n-2)}, \dots, \lambda c^{-1}, 1)$ is an hyperinvariant subspace.*

Proposition 3.6. *Let F be an invariant subspace of $A_{a,c}$. Then it is hyperinvariant.*

Proof. It suffices from Proposition 3.3 that for all $X_{a,c} \in \mathcal{C}(A_{a,c})$ then

$$\begin{aligned} &X_{a,c} = \\ &x_1 I + \frac{x_2}{c}A_{a,c} + \frac{x_3}{c^2}A^2_{a,c} + \dots + \\ &\quad \frac{x_{n-1}}{c^{n-2}}A^{n-2}_{a,c} + \frac{x_n}{c^{n-2}}A^{n-1}_{a,c}. \end{aligned}$$

3.2 Two-parametric Quasi-Cyclic Codes

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

Definition 3.1. *Let a, c be two nonzero elements of $\mathbb{F}$. A code C with length n over the field $\mathbb{F}$ is called generalized constancyclic code if whenever $c = (a_1, \dots, a_n)$ is in C, so is $sc = (a \cdot a_n, a_1, c \cdot a_2 \dots, c \cdot a_{n-1})$.*

As immediate consequence of definition we have the following Proposition.

Proposition 3.7. *A linear code C with length n over the field $\mathbb{F}$ is generalized constancyclic if, and only if, C is an $A_{a,c}$-invariant subspace of $\mathbb{F}^n$.*

After Proposition 3.6 we have the following result.

Proposition 3.8. *A linear code C with length n over the field $\mathbb{F}$ is two-parameter cyclic if, and only if, C is a $A_{a,c}$-hyperinvariant subspace of $\mathbb{F}^n$.*

Suppose now that $(n, q) = 1$ and $p_{a,c}(s) = (-1)^n(s^n - c^{n-2}a)$ has no multiple roots and splits into distinct irreducible monic factors.

Proposition 3.9. *Let C be generalized constancyclic code, and $p_{a,c}(s) = (-1)^n p_{a,c_1}(s) \cdot \dots \cdot p_{a,c_r}(s)$ the decomposition of $p_{a,c}(s)$ in irreducible factors. Then $C = \operatorname{Ker} p_{a,c_{i_1}}(A_{a,c}) \oplus \dots \oplus \operatorname{Ker} p_{a,c_{i_s}}(A_{a,c})$ for some minimal $A_{a,c}$-invariant subspaces $\operatorname{Ker} p_{a,c_{i_j}}(A_{a,c})$ of $\mathbb{F}^n$.*

Proof. First, it is easy to see that $\operatorname{Ker} p_{a,c_i}(A_{a,c})$ for $i = 1, \dots, r$ are $A_{a,c}$-invariant: let $v \in \operatorname{Ker} p_{a,c_i}(A_{a,c})$ then $A_{a,c}v = p_{a,c_1}(A_{a,c}) \cdot \dots \cdot p_{a,c_r}(A_{a,c})v = 0$.

The subspaces $\operatorname{Ker} p_{a,c_{i_j}}(A_{a,c})$ are minimal because the polynomials $p_{a,c_i}(s)$ are irreducible.

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

Let $x \in C$, then $x = q_1(A_{a,c})\widehat{p}_1(A_{a,c})x + \dots + q_r(A_{a,c})\widehat{p}_r(A_{a,c})x$. Calling $x_i = q_i(A_{a,c})\widehat{p}_i(A_{a,c})x$ and taking into account that C is $A_{a,c}$-invariant, and that $x_i \in \operatorname{Ker} p_{a,c_i}(A_{a,c})$ we have that $x_i \in C \cap \operatorname{Ker} p_{a,c_i}(A_{a,c})$.

Example 3.1. *Consider the matrix $A_{a=2,c=4}$ for $n = 8$, $q = 5$. Then we have $p(s) = p_{a=2,c=4}(s) = s^8 - 1$. Factorizing $p(s)$ into irreducible factors over $\mathbb{F} = GF(5)$ 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 $A_{a,c}$-invariant subspaces $F_i = \operatorname{Ker} p_i(A_{a,c})$, for $i = 1, 2, 3, 4, 5, 6$.*

We define a generalized constancyclic linear code $C_{a,c}$ by

$$C_{a,c} = F_1 \oplus F_5 = \operatorname{Ker}(p_1(A_{a,c})) \oplus \operatorname{Ker}(p_5(A_{a,c}))$$

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

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

$$\begin{aligned} &\operatorname{Ker}(A^3_{a,c} + A^2_{a,c} + 2A_{a,c} + 2I) = \\ &[(1,4,2,1,3,4,2,1), (1,0,4,0,2,0,1,0), \\ &\quad (0,3,0,4,0,2,0,1)]. \end{aligned}$$

3.3 Particular Case: $b = c = 1$

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

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

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

This linear map verifies $A_a^{-1} = A_{1/a}^t$. The characteristic polynomial is

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

Proposition 3.10. *The centralizer $\mathcal{C}(A_a)$ of A_a is the set of matrices*

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

Proof. Is a particular case of Proposition 3.1.

Remark 3.1. *If $X_a \in \mathcal{C}(A_a)$ then $X_a^t \in \mathcal{C}(A_{1/a})$. For that, it suffices to observe suffices to observe that*

$$X_a^t = \begin{pmatrix} x_1 & \frac{1}{a}x_n & \dots & \frac{1}{a}x_3 & \frac{1}{a}x_2 & \\ x_2 & x_1 & \dots & \frac{1}{a}x_{n-3} & \frac{1}{a}x_{n-2} & \\ x_3 & x_2 & \dots & \frac{1}{a}x_{n-3} & \frac{1}{a}x_{n-2} & \\ \vdots & \vdots\vdots & \vdots & \ddots & \vdots & \vdots \\ x_n & x_{n-1} & \dots & x_2 & x_1 & \end{pmatrix} \in \mathcal{C}(A_{1/a})$$

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

Proposition 3.11. *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 $(w')^t = X^t w^t$ then, we have:

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

and then $X^t w^t = (w')^t \in F^\perp$ 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 $v = (v_1, \dots, v_n)$ is an eigenvector of A_a, then the following equalities hold:

$$\begin{aligned} av_n &= \lambda v_1 \\ v_1 &= \lambda v_2 \\ &\dots \\ v_{n-2} &= \lambda v_{n-1} \\ v_{n-1} &= \lambda v_n \end{aligned} \qquad (6)$$

In particular, we obtain that

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

and we have the following Proposition.

Proposition 3.12. *Given any $\lambda \in GF(q)^*$ such that $\lambda^n = a$, then $[v] = [(\lambda^{n-1}, \lambda^{n-2}, \dots, \lambda, 1)]$ is an hyperinvariant subspace.*

Proposition 3.13. *Let F be an invariant subspace of A_a. Then it is hyperinvariant.*

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

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

Example 3.2. *Over $\mathbb{F} = GF(5)$ we consider*

$$A_2 = \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$F = [(1, 2, 4)]$ 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 with $b = c$

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

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

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

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

3.4 Constacyclic Codes

A particular case of generalized constacyclic codes are constancyclic codes which were introduced in [Berlekamp, 1968].

Definition 3.2. *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 and Van-Zanten, 2009], we have the following Propositions.

Proposition 3.14. *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 3.15. *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 3.13 we deduce the following result.

Proposition 3.16. *A linear code C with length n over the field $\mathbb{F}$ is constacyclic if and only if C is an A_a-hyperinvariant subspace of $\mathbb{F}^n$.*

Example 3.3. *Consider the matrix $A_{a=4}$ for $n = 8$, $q = 5$. 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*

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

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

References

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

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

Garcia-Planas M.I., Soudi El M., and Um L.E., (2012). *Analysis of control properties of concatenated convolutional codes*. Cybernetics and Physics. 1(4), pp. 252–257.

Garcia-Planas, M.I., Soudi, El M., and 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., and Schmale, W., (2004) *On Cyclic Convolutional Codes*. Acta Applicandae Mathematicae, 82, pp. 183–237.

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

Radkova, D., Bojilov, A., and Van Zanten, A.J., (2007). *Cyclic Codes and Quasi-Twisted Codes: an Algebraic Approach*. Report MICC 07-08, Universiteit Maastricht.

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