Open Mathematics

Research Article

María Isabel García-Planas*, Maria Dolors Magret, and Laurence Emilie Um

Monomial codes seen as invariant subspaces

https://doi.org/10.1515/math-2017-0093
Received May 2, 2016; accepted May 17, 2017.

Abstract: It is well known that cyclic codes are very useful because of their applications, since they are not computationally expensive and encoding can be easily implemented. The relationship between cyclic codes and invariant subspaces is also well known. In this paper a generalization of this relationship is presented between monomial codes over a finite field $\mathbb{F}$ and hyperinvariant subspaces of $\mathbb{F}^n$ under an appropriate linear transformation. Using techniques of Linear Algebra it is possible to deduce certain properties for this particular type of codes, generalizing known results on cyclic codes.

Keywords: Monomial codes, Invariant subspaces

MSC: 94B15, 15B33

1 Introduction

It is well known that error correcting codes and cryptographic systems have conflicting objectives, since the first are codes protecting the information of occasional errors due to handling, that is, those searching to solve the difficulties posed by unreliability of the channel, but cryptosystems, also called secret codes, try to ensure its confidentiality, integrity and security. However, they also have complementary objectives. The difficulty for decoding error correcting codes has been used to build cryptographic systems from these codes. Among these systems there is the well known public key McEliece system. In this system the private key of each user is the generator matrix G of a linear code C over a finite field $\mathbb{F}_q$ joint with a decoding algorithm. The matrix G is hidden by a permutation matrix thus obtaining the public key, ([1], [2], [3]).

Alongside the use of cryptography to protect communications, there is the technique known as "steganography"whose use is increasing and which consists in the concealment of information. It is used in order to protect information in an anodyne numerical support and it is the support that is sent over a public transmission channel. These techniques of concealment of information are based on cyclic codes over the ring $\mathbb{Z}_4$, ([4], [5]). Possibly they can improve the efficiency in dissimulation using a generalization of cyclic codes such as the monomial codes.

A first generalization of cyclic codes were constacyclic codes, introduced by E. R. Berlekamp in [6]. Monomial codes are a broader generalization. Linear algebra as a tool to study such codes was introduced in [7]. Monomial codes are widely used because they can be encoded with shift registers.

Let p be a prime number, $q = p^k$ for some $k \geq 1$. A monomial q-ary code of length n can be defined through a $n \times n$ generator-matrix with the property that each row (except the last one) $(c_1, c_2, \ldots, c_n)$, $c_i \in GF(q)$ defines the row as $(a_n c_n, a_1 c_1, a_2 c_2, \ldots, a_{n-1} c_{n-1})$, where $a_1, \ldots, a_n$ are certain fixed elements of $GF(q)\backslash\{0\}$. Cyclic codes $(a_1 = \ldots = a_n = 1)$ and constacyclic codes $(a_1 = \ldots = a_{n-1} = 1)$ are special subclasses of monomial codes of $GF(q)^n$. Monomial codes can also be described in terms of linear algebra, which constitutes our starting

***Corresponding Author: María Isabel García-Planas:** Universitat Politècnica de Catalunya, Spain
Maria Dolors Magret: Universitat Politècnica de Catalunya, Spain, E-mail: m.dolors.magret@upc.edu
Laurence Emilie Um: Université Mohammed V-Agdal, Morocco, E-mail: laurence.um@gmail.com

point that will be the characteristic polynomial of the endomorphism of $GF(q)^n$ whose matrix in the canonical basis is the one representing the monomial code.

Recall that, given an endomorphism φ of a $\mathbb{F}$-vector space E, a φ-invariant subspace $V \subset E$ is hyperinvariant when it is invariant under all linear transformations commuting with φ.

2 Invariant subspaces of monomial matrices

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

Let $\overline{a} = (a_1, \dots a_n)$ be a set of n parameters of $\mathbb{F}$ and consider the following linear map

$$\begin{aligned} \varphi_{\overline{a}} : \mathbb{F}^n &\longrightarrow \mathbb{F}^n \\ (x_1, \dots, x_n) &\longrightarrow (a_n x_n, a_1 x_1, \dots, a_{n-1} x_{n-1}) \end{aligned} \tag{1}$$

whose associated matrix with respect to the canonical basis $\{e_1 = (1, 0, \dots, 0), e_2 = (0, 1, \dots, 0), e_n = (0, 0, \dots, 1)\}$ is:

$$A_{\overline{a}} = \begin{pmatrix} 0 & 0 & \dots & 0 & a_n \\ a_1 & 0 & \dots & 0 & 0 \\ 0 & a_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_{n-1} & 0 \end{pmatrix}. \tag{2}$$

This matrix is called a monomial matrix. We note that this matrix can be written as the product of a diagonal matrix diag $(a_n, a_1, \dots, a_{n-1})$ and the permutation matrix

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

Properties

This matrix verifies:

1) $A_{\overline{a}}^n = a_1 \dots a_n I_n$
2) if $\prod_{i=1}^n a_i \neq 0$ then $A_{\overline{a}}^{-1} = \frac{1}{\prod_{i=1}^n a_i} A_{\overline{a}}^{n-1} = A_{\overline{\overline{a}}}^t$, where $\overline{\overline{a}} = (\frac{1}{a_1}, \dots, \frac{1}{a_n})$.
3) its characteristic polynomial is $p_a(s) = \det(A_{\overline{a}} - sI_n) = (-1)^n (s^n - \prod_{i=1}^n a_i)$.

Proposition 2.1. *Suppose that $a = \prod_{i=1}^n a_i \neq 0$. Then, the matrix* (2) *is equivalent under similarity to*

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

Proof. It is easy to prove that

$$A_{\overline{a}} S = S A_a.$$

with

$$= \begin{pmatrix} 0 & 0 & \dots & 0 & \prod_{i=1}^n a_i \\ a_1 & 0 & \dots & 0 & 0 \\ 0 & a_1 a_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & \prod_{i=1}^{n-1} a_i & 0 \end{pmatrix}$$

□

In this section we prove that a $\varphi_{\overline{a}}$-invariant subspaces are also $\varphi_{\overline{a}}$-hyperinvariants; that is to say, invariant under all linear maps commuting with $\varphi_{\overline{a}}$, (see [8] and [9] for more information about these subspaces).

We need to know the centralizer of $A_{\overline{a}}$. To do that, we first calculate the centralizer of the matrix A_a.

Proposition 2.2 ([7]**.** *] The centralizer $\mathcal{C}(A_a)$ is the set of the matrices X_a in the form:*

$$X_a = \begin{pmatrix} x_n & ax_1 & ax_2 & ax_3 & \dots & ax_{n-2} & ax_{n-1} \\ x_{n-1} & x_n & ax_1 & abx_2 & \dots & ax_{n-3} & ax_{n-2} \\ \vdots & & \ddots & \ddots & & & \\ \vdots & & & \ddots & \ddots & & \\ x_3 & x_4 & x_5 & x_6 & \dots & ax_1 & ax_2 \\ x_2 & x_3 & x_4 & x_5 & \dots & x_n & ax_1 \\ x_1 & x_2 & x_3 & x_4 & \dots & x_{n-1} & x_n \end{pmatrix}$$

Proposition 2.3. *The centralizer $\mathcal{C}(A_{\overline{a}})$ of $A_{\overline{a}}$ is the set of the matrices $Y_{\overline{a}} = SX_aS^{-1}$, if $A_{\overline{a}}S = SA_a$.*

Proof. Proposition 2.2, we have $X_aA_a = A_aX_a$. Then, $SX_aS^{-1}A_{\overline{a}} = A_{\overline{a}}SX_aS^{-1}$. □

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

$$\begin{aligned} a_nv_n &= \lambda v_1 \\ a_1v_1 &= \lambda v_2 \\ a_2v_2 &= \lambda v_3 \\ &\vdots \\ a_{n-2}v_{n-2} &= \lambda v_{n-1} \\ a_{n-1}v_{n-1} &= \lambda v_n \end{aligned} \tag{3}$$

In particular, we have that

$$v = \left(\frac{\lambda^{n-1}}{a_1 \dots a_{n-1}}, \frac{\lambda^{n-2}}{a_2 \dots a_{n-1}}, \dots, \frac{\lambda}{a_{n-1}}, 1\right) \tag{4}$$

and the following Proposition holds.

Proposition 2.4. *Let $\lambda \in GF(q)^*$ be an element such that $\lambda^n = \prod_{i=1}^n a_i$. Then, the one-dimensional subspace $[v]$ spanned by the vector v given in (4) is an hyperinvariant subspace.*

Proof.

$$A_{\overline{a}}v = \lambda v$$

and given any $Y_{\overline{a}} \in \mathcal{C}(A_{\overline{a}})$, then

$$\begin{aligned} & Y_{\overline{a}}v = \\ & S(x_nI + x_{n-1}A_{\overline{a}} + x_{n-2}A_{\overline{a}}^2 + \dots + x_1A_{\overline{a}}^{n-1})S^{-1}v \\ & = x_nv + x_{n-1}SA_aS^{-1}v + x_{n-2}SA_a^2S^{-1}v + \dots + \\ & + x_2SA_a^{n-2}S^{-1}v + x_1SA_{\overline{a}}^{n-1}S^{-1}v \\ & = x_nv + x_{n-1}\lambda v + x_{n-2}\lambda^2v + \dots + x_1\lambda^{n-1}v \\ & = \alpha v \end{aligned}$$

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

Proposition 2.5. *Let F be an invariant subspace of $A_{\overline{a}}$. Then, F is hyperinvariant.*

Proof. It suffices to observe that, for all $Y_{\overline{a}} \in \mathcal{C}(A_{\overline{a}})$,

$$SX_aS^{-1} = x_nI + x_{n-1}A_{\overline{a}} + x_{n-2}A_{\overline{a}}^2 + \dots + x_1A_{\overline{a}}^{n-1}.$$

□

Therefore, in this case the lattice of invariant subspaces coincides with the lattice of hyperinvariant subspaces:

$$\operatorname{Hinv}(A_{\overline{a}}) = \operatorname{Inv}(A_{\overline{a}}).$$

Definition 2.6. *i) Let $u = (u_1, \dots, u_n)$ and $v = (v_1, \dots, v_n)$ be two vectors in $\mathbb{F}^n$. We define an inner product over $\mathbb{F}$ as follows:*

$$< u, v >= u_1 v_1 + \ldots + u_n v_n.$$

ii) Two vectors u, v in $\mathbb{F}^n$ are said to be orthogonal if $< u, v >= 0$.

iii) Let F be a subspace of $\mathbb{F}^n$. The dual subspace of F (denoted by $F^\perp$) is

$$F^\perp = \{v \in \mathbb{F}^n \mid \forall u \in F, \ < u, v >= 0\}.$$

Proposition 2.7. *Let F be an invariant subspace of $A_{\overline{a}}$. Then $F^\perp$ is an invariant subspace of $A_{\overline{a}}^{-1}$.*

Proof. Let $v \in F^\perp$. For all $u \in F$ (consequently, $A_{\overline{a}} u \in F$) we have

$$\begin{aligned} 0 &=< A_{\overline{a}} u, v >=< u, A_{\overline{a}}^t v >=< u, \textstyle\prod_{i=1}^n a_i A_{\overline{a}}^{n-1} v > \\ &=< u, A_{\overline{a}}^{-1} v > \end{aligned}$$

Thus $A_{\overline{a}}^{-1} v \in F^\perp$. □

Let $\mathbb{F}[\lambda_1, \dots, \lambda_n]$ be the algebraic extension of $\mathbb{F} = GF(q)$ and let $\lambda_1, \dots, \lambda_n$ be the eigenvalues of $\varphi_{\overline{a}}$ with $\lambda_i = \sqrt[n]{\prod_{i=1}^n \lambda^i}$, $i = 1, \dots, n$, where λ is a primitive n^{th} root of unity and $\sqrt[n]{\prod_{i=1}^n a_i}$ is a fixed, but otherwise arbitrary zero of the polynomial $s^n - \prod_{i=1}^n a_i$, where $0 \neq \prod_{i=1}^n a_i \in \mathbb{F}$.

Let v_i, $i = 1, \dots, n$ be the respective eigenvectors. More particularly we have

$$A_{\overline{a}} v_i = \lambda_i v_i, \ v_i = \left(\frac{\lambda_i^{n-1}}{a_1 \ldots a_{n-1}}, \frac{\lambda_i^{n-2}}{a_2 \ldots a_{n-1}}, \dots, \frac{\lambda_i}{a_{n-1}}, 1 \right),$$

$i = 1, \dots, n$,
where $A_{\overline{a}}$ is the matrix associated to

$$\varphi_{\overline{a}} : \mathbb{F}[\lambda_1, \dots, \lambda_n]^n \longrightarrow \mathbb{F}[\lambda_1, \dots, \lambda_n]^n$$

(defined as in 2).

Let us consider the basis $v = (v_1, \dots, v_n)$ of eigenvectors of $\varphi_{\overline{a}}$. Applying basis change to $A_{\overline{a}}$, we obtain the following diagonal matrix

$$D_{\overline{a}} = \begin{pmatrix} \lambda_1 & 0 & \ldots & 0 \\ 0 & \lambda_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \lambda_n \end{pmatrix} = S^{-1} A S$$

and taking into account (4) we have

$$S = \begin{pmatrix} \frac{\lambda_1^{n-1}}{a_1 \ldots a_{n-1}} & \frac{\lambda_2^{n-1}}{a_1 \ldots a_{n-1}} & \ldots & \frac{\lambda_n^{n-1}}{a_1 \ldots a_{n-1}} \\ \frac{\lambda_1^{n-2}}{a_2 \ldots a_{n-1}} & \frac{\lambda_2^{n-2}}{a_2 \ldots a_{n-1}} & \ldots & \frac{\lambda_n^{n-2}}{a_2 \ldots a_{n-1}} \\ \vdots & \vdots & & \vdots \\ \frac{\lambda_1}{a_{n-1}} & \frac{\lambda_2}{a_{n-1}} & \ldots & \frac{\lambda_n}{a_{n-1}} \\ 1 & 1 & \ldots & 1 \end{pmatrix}$$

We define now the following vectors:

$$\begin{aligned} &u_i = (\lambda_i a_1 \ldots a_{n-1}, \lambda_i^2 a_2 \ldots a_{n-1}, \dots, \lambda^{n-1} a_{n-1}, \lambda_i^n), \\ &1 \le i \le n \end{aligned} \tag{5}$$

Proposition 2.8. *The set of vectors defined in* (5) *verify the following relationship.*

$$< u_i, v_j >= \begin{cases} a_1 \dots a_n n \text{ if } i = j \\ 0 \qquad\quad \text{if } i \neq j \end{cases}$$

Proof.

$$< u_i, v_j >= \sum_{\ell=1}^n \lambda_i^\ell \lambda_j^{n-\ell} = \sum_{\ell=1}^n \frac{\lambda_i^\ell \lambda_j^{n-\ell} \lambda_j^\ell}{\lambda_j^\ell} =$$
$$\sum_{\ell=1}^n \left(\frac{\lambda_i}{\lambda_j}\right)^\ell \lambda_j^n = a_1 \dots a_n \sum_{\ell=1}^n \left(\frac{\lambda_i}{\lambda_j}\right)^\ell =$$
$$\begin{cases} a_1 \dots a_n \sum_{\ell=1}^n 1^\ell = a_1 \dots a_n n \text{ if } i = j \\ a_1 \dots a_n \sum_{\ell=1}^n (\lambda)^\ell = 0 \text{ (with } \lambda \text{ a root of unit) if } i \neq j \end{cases}$$

□

From this Proposition the inverse matrix of the matrix S can easily obtained.

3 Monomial codes as invariant subspaces

Definition 3.1. *A code C of length n over the field $\mathbb{F}$ is called monomial with respect to $a_1, \dots, a_n$, if whenever $c = (c_1, \dots, c_n)$ belongs to C, then $sc = (a_n c_n, a_1 c_1, \dots, a_{n-1} c_{n-1})$ is also in C.*

The shift (the map $c \to sc$) can be represented in a matrix form

$$\begin{pmatrix} 0 & 0 & \dots & 0 & a_n \\ a_1 & 0 & \dots & 0 & 0 \\ 0 & a_2 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & a_{n-1} & 0 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} a_n c_n \\ a_1 c_1 \\ a_2 c_2 \\ \vdots \\ a_{n-1} c_n \end{pmatrix}$$

Note that this matrix is the matrix (2).

In the particular case where $a_i = 1$, for all i, the code is a cyclic code and if $a_1 = \dots = a_{n-1} = 1$ is a constacyclic code (see [10]).

Applying Proposition 2.1 the study can be reduced to the case of constacyclic codes. Nevertheless, we will not make use of this result, but directly consider monomial codes.

We are interested in the case where $a_n \neq a_i$ for some $i = 2, \dots, a_{n-1}$ and $\prod_{i=1}^n a_i \neq 0$. In particular, we need to consider $q > 2$. As an immediate consequence of Definition 3.1 we have the following Proposition.

Proposition 3.2. *A linear code C with length n over the field $\mathbb{F}$ is monomial if, and only if, C is an $A_{\overline{a}}$-invariant subspace of $\mathbb{F}^n$.*

And after Proposition 2.5 we have the following result.

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

Suppose now that $(n, q) = 1$ and $p_{\overline{a}}(t) = (-1)^n (t^n - \prod_{i=1}^n a_i)$ has no multiple roots and splits into distinct irreducible factors.

General Linear Algebra theory over finite fields yields the following statement.

Proposition 3.4. *Let C be a monomial code, and*

$$p_{\overline{a}}(s) = (-1)^n p_{\overline{a}_1}(s) \cdot \dots \cdot p_{\overline{a}_r}(s)$$

the decomposition of $p_{\overline{a}}(s)$ into irreducible factors. Then $C = \operatorname{Ker} p_{\overline{a}_{i_1}}(A_{\overline{a}}) \oplus \dots \oplus \operatorname{Ker} p_{\overline{a}_{i_s}}(A_{\overline{a}}) = \operatorname{Ker} h(A_{\overline{a}})$, $h(s) = p_{\overline{a}_{i_1}}(s) : . : p_{\overline{a}_{i_t}}(s)$ for some minimal $A_{\overline{a}}$-invariant subspaces $\operatorname{Ker} p_{\overline{a}_{i_j}}(A_{\overline{a}})$ de $\mathbb{F}^n$.

Example 3.5. *Consider the matrix $A_{\overline{a}}$ with $a_n = 2, a_1 = 4$, $a_2 = \ldots = a_{n-1} = 1$, $n = 8$ and $q = 5$. Then $p(s) = p_{\overline{a}}(s) = s^8 - 1$. Factorizing $p(s)$ into irreducible factors over $\mathbb{F} = GF(5)$ we have $p_{\overline{a}}(s) = p_1(s)p_2(s)p_3(s)p_4(s)p_5(s)p_6(s) = (s+1)(s+2)(s+3)(s+4)(s^2+2)(s^2+3)$. The factors $p_i(s)$ define minimal $A_{\overline{a}}$-invariant subspaces, $F_i = \operatorname{Ker} p_i(A_{\overline{a}})$, for $i = 1,2,3,4,5,6$.*

Let us consider
$C = F_1 \oplus F_5 = \operatorname{Ker}(p_1(A_{\overline{a}})) \oplus \operatorname{Ker}(p_5(A_{\overline{a}}))$
$\operatorname{Ker}(A_{\overline{a}}^3 + A_{\overline{a}}^2 + 2A_{\overline{a}} + 2I) =$

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

This is a monomial code, $C = \operatorname{Ker} h(A_{\overline{a}})$ with $h(s) = p_1(s)p_5(s) = s^3 + s^2 + 2s + 2$.

Example 3.6. *With the notations as in the Example above,*

$$g(s) = \frac{P_{\overline{a}}(s)}{h(s)} = p_2(s)p_3(s)p_4(s)p_6(s) = s^5 + 9s^4 + 29s^3 + 53s^2 + 78s + 72$$

It is straightforward to check that

$$\begin{array}{l}(A_{\overline{a}}^5 + 9A_{\overline{a}}^4 + 29A_{\overline{a}}^3 + 53A_{\overline{a}}^2 + 78A_{\overline{a}} + 72I)(v_1) = 0\\ (A_{\overline{a}}^5 + 9A_{\overline{a}}^4 + 29A_{\overline{a}}^3 + 53A_{\overline{a}}^2 + 78A_{\overline{a}} + 72I)(v_2) = 0\\ (A_{\overline{a}}^5 + 9A_{\overline{a}}^4 + 29A_{\overline{a}}^3 + 53A_{\overline{a}}^2 + 78A_{\overline{a}} + 72I)(v_3) = 0\end{array}$$

with

$$v_1 = (1,4,2,1,3,4,2,1), v_2 = (1,0,4,0,2,0,1,0), v_3 = (0,3,0,4,0,2,0,1).$$

Corollary 3.7. *Let C be a monomial code. There exists $g(s)$ verifying $p_{\overline{a}}(s) = g(s)\cdot h(s)$ with $gcd(g(s), h(s)) = 1$ such that $g(A_{\overline{a}})c = 0$, $\forall c \in C$.*

Considering the inner product introduced in definition 2.6.

Proposition 3.8. *Let C be a monomial code with respect $a_1, \ldots, a_n$. Then, its dual code $C^\perp$ is a monomial code with respect $\frac{1}{a_1}, \ldots, \frac{1}{a_n}$.*

Proof. The statement follows from Proposition 2.7. □

In the case $a_1 = \ldots = a_n = 1$ we obtain the well known result about cyclic codes.

Corollary 3.9. *The dual of a cyclic code is a cyclic code.*

4 Parity matrices of monomial codes

Let $\mathbb{F}[\lambda_1, \ldots, \lambda_n]$ be the algebraic extension considered in Section 2.

Let C be a monomial code and $g(s)$ as in corollary 3.7. Let us consider a basis $v = (v_1, \ldots, v_n)$ of eigenvectors of $\varphi_{\overline{a}}$.

In this basis, the matrix of $\varphi_{\overline{a}}$ is a diagonal matrix, which will be denoted by $D_{\overline{a}}$.

Since $D_{\overline{a}}$ is a diagonal matrix, the matrix $g(D_{\overline{a}})$ is also diagonal and

$$g(A_{\overline{a}}) = g(SD_{\overline{a}}S^{-1}) = Sg(D_{\overline{a}})S^{-1}$$

Condition $g(A_{\overline{a}})c = 0$ is equivalent to $g(D_{\overline{a}})c' = 0$ where $c' = S^{-1}c$.

Without loss of generality we can assume that $\lambda_1, \dots, \lambda_n$ are ordered in such a way that $g(\lambda_i) = 0$, for all $1 \leq i \leq k$ and $g(\lambda_i) = \alpha_i \neq 0$, for all $k+1 \leq i \leq n$. With $h(s)$ as in corollary 3.7, $h(\lambda_i) \neq 0$, for all $1 \leq i \leq k$ and $h(\lambda_i) = 0$, for all $k+1 \leq i \leq n$. Given $c = (c_1, \dots, c_n) \in C$ and $c' = (c'_1, \dots, c'_n) = s^{-1}c$ we have that $g(D_{\overline{a}}) = (0, \dots, 0, \alpha_{k+1}c'_{k+1}, \dots, \alpha_n c'_n)$. Equivalently:

$$\frac{1}{a_1 \dots a_n n}\begin{pmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ & & & \alpha_{k+1} & & \\ & & & & \ddots & \\ & & & & & \alpha_n \\ & & & & 0 & \end{pmatrix}\begin{pmatrix} \lambda_1 a_1 \dots a_{n-1} & \lambda_1^2 a_2 \dots a_{n-1} & \dots & \lambda_1^{n-1} a_{n-1} & \lambda_1^n \\ \lambda_2 a_1 \dots a_{n-1} & \lambda_2^2 a_2 \dots a_{n-1} & \dots & \lambda_2^{n-1} a_{n-1} & \lambda_2^n \\ \vdots & \vdots & & \vdots & \vdots \\ \lambda_n a_1 \dots a_{n-1} & \lambda_n^2 a_2 \dots a_{n-1} & \dots & \lambda_n^{n-1} a_{n-1} & \lambda_n^n \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$$

$$= \frac{1}{a_1 \dots a_{n-1} n}\begin{pmatrix} & \ddots & & \\ & & 0 & \\ \alpha_{k+1}\lambda_{k+1} a_1 \dots a_{n-1} & & & \dots \alpha_{k+1}\lambda_{k+1}^n \\ \vdots & & & \vdots \\ \alpha_n \lambda_n a_1 \dots a_{n-1} & & \dots & \alpha_n \lambda_n^n \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix} = 0$$

Then we can deduce the following proposition.

Proposition 4.1. *Let u_{i_j}, $1 \leq j \leq r = n-k$ be a family of vectors as in* (5) *corresponding to λ_{i_j}, with $g(\lambda_{i_j}) = \alpha_{i_j} \neq 0$. Then c is a codeword of the monomial code C if and only if*

$$u_{i_j}c = 0, \textit{ for all } 1 \leq j \leq r.$$

As a consequence the matrix $A = (u_{i_j}) \in M_{(n-k)\times n}(\mathbb{F}[\lambda_1, \dots, \lambda_n])$ is a parity matrix of the monomial code over the field $\mathbb{F}[\lambda_1, \dots, \lambda_n]$.

Example 4.2. *Over $\mathbb{F} = GF(5)$ we consider a monomial code C with $a_n = a_1 = 2$, $a_2 = \dots = a_{-1} = 1$ and $n = 4$ defined by $g(s) = s^2 - 2$. Over $\mathbb{F}[\sqrt{2}, 4\sqrt{2}, \sqrt{3}, 4\sqrt{3}]$, the polynomial $h(s) = s^2 + 2 = (s - \sqrt{3})(s - 4 \cdot \sqrt{3})$. Then*

$$\begin{pmatrix} \sqrt{3}\cdot 2 & 3 & 3\cdot\sqrt{3} & 4 \\ 3\cdot\sqrt{3} & 3 & 2\cdot\sqrt{3} & 4 \end{pmatrix}$$

is a parity matrix of the code C over $\mathbb{F}[\sqrt{2}, 4\sqrt{2}, \sqrt{3}, 4\sqrt{3}]$.

5 Hamming distance of monomial codes

Remember that the Hamming weight (for short, weight) of a vector v is the number of its nonzero entries and is denoted $w_H(v)$. We have $w_H(x) = d_H(x, 0)$. The minimum weight of a code C is the minimum nonzero weight among all codewords of C,

$$w_{\min}(C) = \min_{0 \neq x \in C}(w_H(x))$$

Taking into account that $d_H(x, y) = d_H(x-z, y-z)$ for all z and that in particular $d_H(x, y) = d_H(x-y, y-y) = d_H(x-y, 0)$ we have that over a field, the Hamming distance is translation invariant and, in particular, for linear codes, the minimum weight is equal to the minimum distance.

We are going to obtain a bound for the minimum distance of two parametric monomial codes in a similar way to that presented by Roos in [11] for cyclic codes.

Let $\mathbb{F}$ be a finite field and

$$A = \begin{pmatrix} \mathbf{a}_1 & \dots & \mathbf{a}_n \end{pmatrix} = \begin{pmatrix} a_{11} & \dots & a_{n1} \\ \vdots & & \vdots \\ a_{1\ell} & \dots & a_{n\ell} \end{pmatrix}.$$

Let C be a linear code over $\mathbb{F}$ having A as a parity matrix and $d_H(A)$ the minimum distance of C.

Remember that $d_H(A) = d$ if and only if every set of $d-1$ columns is linearly independent and some set of d columns of A is linearly dependent.

For any matrix $X = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ \vdots & & \vdots \\ x_{m1} & \dots & x_{mn} \end{pmatrix}$ with nonzero columns $\mathbf{x}_i \in \mathbb{F}^m$ for $1 \leq i \leq n$ we consider

$$A(X) = \begin{pmatrix} \mathbf{x}_1 \otimes \mathbf{a}_1 & \dots & \mathbf{x}_n \otimes \mathbf{a}_n \end{pmatrix}$$

The following result is well known due to Roos ([12]).

Lemma 5.1. *If $d_H(A) \geq 2$ and every $m \times (m + d_H(A) - 2)$ submatrix of X has full rank, then $d_H(A(X)) \geq d_H(A) + m - 1$.*

Definition 5.2. *Let $M = [\lambda_{i_1}, \dots, \lambda_{i_\ell}]$ be a set of ℓ roots of $s^n - \prod_{i=1}^n a_i$ in $\mathbb{F}[\lambda_1, \dots, \lambda_n]$. We will say that M is a consecutive set of length ℓ, if there exists a primitive n-root of the unit λ and an exponent i such that $M = [\sqrt[n]{\prod_{i=1}^n a_i}\lambda^i, \dots, \sqrt[n]{\prod_{i=1}^n a_i}\lambda^{i+\ell-1}]$.*

Definition 5.3. *a) Let $\Lambda = [\lambda_{j_1}, \dots, \lambda_{j_\ell}]$ be a set of zeros of the polynomial $s^n - \prod_{i=1}^n a_i$. We define the matrix*

$$A_\Lambda = \begin{pmatrix} \lambda_{j_1} a_1 \dots a_{n-1} & \lambda_{j_1}^2 a_2 \dots a_{n-1} & \dots & \lambda_{j_1}^n \\ \vdots & \vdots & & \vdots \\ \lambda_{j_\ell} a_1 \dots a_{n-1} & \lambda_{j_\ell}^2 a_2 \dots a_{n-1} & \dots & \lambda_{j_\ell}^n \end{pmatrix} \in M_{\ell \times n}(\mathbb{F}[\lambda_1, \dots, \lambda_n]).$$

b) Let $U = [x_1, \dots, x_m]$ be a set of consecutive zeros of the polynomial $s^n - 1$. We define the matrix

$$X_U = \begin{pmatrix} x_1 & x_1^2 & \dots & x_1^n \\ \vdots & \vdots & & \vdots \\ x_m & x_m^2 & \dots & x_m^n \end{pmatrix} \in M_{m \times n}(\mathbb{F}[\lambda_1, \dots, \lambda_n]).$$

Let C be the monomial code defined by the polynomial $p_{\overline{a}}(s) = g(s) \cdot h(s)$ over the splitting field $\mathbb{F}[\lambda_1, \dots, \lambda_n]$ of $p_{\overline{a}}(s)$ and consider now as Λ the set of all zeros of $h(s)$. Following 4.1 the matrix A_Λ is a parity matrix of the code C, if the minimum distance of C over $\mathbb{F}[\lambda_1, \dots, \lambda_n]$ is $d_H(A_\Lambda)$. Then, the minimum distance of C over $\mathbb{F}$ is at least $d_H(A_\Lambda)$, since C over $\mathbb{F}$ is a subfield subcode of C over $\mathbb{F}[\lambda_1, \dots, \lambda_n]$.

Remark 5.4. *Notice that the minors of A_Λ are of Vandermonde type.*

Theorem 5.5. *Let Λ be the set defined in 5.3 and U be a consecutive set of roots of $s^n - 1$ such that $d_H(A_\Lambda) - 2 \geq 0$. Then, $d_H(A_\Lambda(X_U)) \geq d_H(A_\lambda) + \operatorname{card} U - 1$.*

Proof. It suffices to observe that in this particular setup $d_H(A_\Lambda) \geq 2$, then we can apply Lemma 5.1. □

As a Corollary we obtain the following result.

Theorem 5.6. *Let C be a monomial code of length n over $\mathbb{F}$, and $p_{\overline{a}} = g(s)h(s)$. For some integers $\ell, m \geq 1$, suppose that $h(s)$ has a string of m consecutive zeros: $h(\lambda_\ell) = h(\lambda_{\ell+1}) = \ldots = h(\lambda_{\ell+m-1}) = 0$. Then, the minimum distance of C is at least d.*

Example 5.7. *Let $n = 9$, $q = 7$, $a_n = 2$, $a_1 = 3$, $a_2 = \ldots = a_{n-1} = 1$ and let α be a 18th-primitive root of unity. Taking into account that $(x^{18} - 1) = (x^9 - 1)(x^9 + 1)$, α is a root of $x^9 + 1$ and $\alpha^2 = \beta$ is a primitive root of $x^9 - 1$. We want to classify the zeros with respect to the various irreducible polynomial divisors of $x^9 + 1$. We will determine the cyclotomic cosets of 7 modulo 18 containing the odd integers: $C_1 = [1, 7, 13]$, $C_3 = [3]$, $C_5 = [5, 17, 11]$, $C_9 = [9]$, $C_{15} = [15]$.*

Let the zeros of $h(s)$ be α^i with $i \in C_1 \cup C_5$, so $h(s) = (s-\alpha)(s-\alpha^7)(s-\alpha^{13})(s-\alpha^5)(s-\alpha^{17})(s-\alpha^{11})$. Given that $\beta_i = \alpha\beta^i = \alpha^{2i+1}$ the zeros of $h(s)$ can be written as β_2, β_3; β_5, β_6; β_8, β_9. Since $h(s)$ has a string of two consecutive zeros. Then, the two parametric monomial code has a minimum distance $d \geq 3$.

References

[1] McEliece R.J., A public key cryptosystem based on algebraic coding theory. DNS Progress Report, Jet Propulsion Laboratory-California Inst. Of Tech, 1978, 42-44.

[2] Martínez Moro E., Munuera Gómez C., Un Sistema criptográfico de clave pública a partir de códigos correctores en Avances en criptología y seguridad de la información, Directores B. Ramos Álvarez, A. Ribagorda Garnacho, 2004, 125-130.

[3] Celikel Cankaya E., Nair S., Cankaya H.C., Applying error correction codes to achieve security and dependability, *Computer Standards & Interfaces*, 2013, 35, 78-86.

[4] Jouhari H., Souidi El M., A New Steganographic Scheme based on First Order Reed Muller Codes, in Proceedings of the International Conference on Security and Cryptography, Sevilla, Spain, 2011, 351-356.

[5] Jouhari H., Souidi El M., Application of Cyclic Codes over $\mathbb{Z}_4$ in Steganography, *Journal of Applied Mathematical Sciences*, 2012, 6 (139).

[6] Berlekamp E.R., “Algebraic Coding Theory”, Mc Graw-Hill, NewYork, 1968.

[7] Garcia-Planas M.I., Magret M.D., Montoro M.E., Cyclic Codes as Hyperinvariant Subspaces, Proceedings of 6th International Conference on Physics and Control (PhysCon 2013), 2013.

[8] Astuti P., Wimmer H.K., Characteristic and hyperinvariant subspaces over the field GF(2), *Linear Algebra and its Applications*, 2013, 438 (4), 1551-1563.

[9] Fillmore P.A., Herrero D.A., Longsta W.E., The hyperinvariant subspace lattice of a linear transformation, *Linear Algebra and its Applications*, 1977, 17(2), 125-132.

[10] Radkova D., Van Zanten A.J., Constacyclic codes as invariant subspaces, *Linear Algebra and its Applications*, 2009, 430, 855-864.

[11] Roos C., “A New Lower Bound for the Minimum Distance of a Cyclic Code”, *IEEE Transactions on Information Theory*, 1983, II-29 (3), 330-332.

[12] Roos C., “A generalization of the BCH bound for cyclic codes, including the Hartmann Tzeng bound, *J. Comb. Theory Ser*, 1982, 33, 229-232.