

On the structure of monomial codes and their generalizations

Research Article

Hassan Ou-azzou, Mustapha Najmeddine, Lhousain Mouatadid,
Oussama Kabbouch

Abstract: In this paper, we are interested in monomial codes with associated vector $a = (a_0, a_1, \dots, a_{n-1})$, introduced in [4], and more generally in linear codes invariant under a monomial matrix $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$ where σ is a permutation and P_σ its associated permutation matrix. We discuss some connections between monomial codes and codes invariant under an arbitrary monomial matrix M . Next, we identify monomial codes with associated vector $a = (a_0, a_2, \dots, a_{n-1})$ by the ideals of the polynomial ring $R_{q,n} := \mathbb{F}_q[x]/\langle x^n - \prod_{i=0}^{n-1} a_i \rangle$, via a special isomorphism $\varphi_{\bar{a}}$ which preserves the Hamming weight and differs from the classical isomorphism used in the case of cyclic codes and their generalizations. This correspondence leads to some basic characterizations of monomial codes such as generator polynomials, parity check polynomials, and others. Next, we focus on the structure of ℓ -quasi-monomial (ℓ -QM) codes of length $n = m\ell$, where on the one hand, we characterize them by the $R_{q,m}$ -submodules of $R_{q,m}^\ell$. On the other hand, ℓ -QM codes are seen as additive monomial codes over the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$. So, as in the case of quasi-cyclic codes [8], we characterize those codes that have $\mathbb{F}_{q^\ell}$ -linear images with respect to a basis of the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$, based on the CRT decomposition. Finally, we show that ℓ -QM codes and additive monomial codes are asymptotically good.

2010 MSC: 94BXX, 94B15, 94B65

Keywords: Additive codes, Monomial codes, Monomial matrix, Cyclic codes, Quasi-cyclic codes, Polycyclic codes

Hassan Ou-azzou, (Corresponding Author); Department of mathematics, ENSAM-Meknes, Moulay Ismail university, Morocco (hassan.ouazzou@edu.umi.ac.ma).

Mustapha Najmeddine; Department of mathematics, ENSAM-Meknes, Moulay Ismail university, Morocco (m.najmeddine@umi.ac.ma).

Lhousain Mouatadid; Department of mathematics, ENSAM-Meknes, Moulay Ismail university, Morocco (enulms@gmail.com).

Oussama Kabbouch; Department of mathematics, ENSAM-Meknes, Moulay Ismail university, Morocco (oussama.kabbouch@gmail.com).

1. Introduction

Due to their rich algebraic structures and the convenience of their implementation in practice, cyclic codes and their generalizations are among the most studied families of linear codes in coding theory. The strong point of cyclic codes and their generalizations is the concept of cyclicity, which permits the use of the polynomial ring in their studies. For more details, we refer the reader to [10, Chapter 4 and 5], and the vast literature on this topic. In [4], the notion of a monomial code with associated vector $a = (a_0, a_2, \dots, a_{n-1})$ was introduced as a linear code in which the monomial shift $(a_{n-1}c_{n-1}, a_0c_0, \dots, a_{n-2}c_{n-2})$ of any codeword $c = (c_0, c_1, \dots, c_{n-1})$ is again a codeword of C . Hence, they are invariant under the right multiplication under a special monomial matrix $A_{\bar{a}}$ (will be defined later). Monomial codes form a generalization of λ -constacyclic codes $a = (1, \dots, 1, \lambda)$, cyclic (and negacyclic) codes $a = (1, \dots, 1, \pm 1)$. In that paper the authors investigated the algebraic structure of monomial codes, based on the theory of invariant subspaces and the irreducible factorization of

$$f_{\bar{a}}(x) = x^n - \prod_{i=0}^{n-1} a_i, \text{ the minimal polynomial of } A_{\bar{a}}.$$

In this paper, we continue the study of monomial codes, in general, the study of codes invariant under a monomial matrix $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_{\sigma}$ where σ is a permutation and P_{σ} its associated permutation matrix. We find that monomial codes are invariant under $A_{\bar{a}} = \text{diag}(a_0, a_1, \dots, a_{n-1})P_{\sigma}$, where σ is an n -cycle of "standard form" (Remark 2.5), and we discuss some connections between monomial codes and codes invariant under an arbitrary monomial matrix. Next, we identify monomial codes with

associated vector $a = (a_0, a_2, \dots, a_{n-1})$ by the ideals of the polynomial ring $R_{q,n} := \mathbb{F}_q[x] / \langle x^n - \prod_{i=0}^{n-1} a_i \rangle$,

via an $\mathbb{F}_q$ -vector space isomorphism $\varphi_{\bar{a}}$ which preserves the Hamming weight and it is different from the classical isomorphism used in the case of cyclic codes and their generalizations. This correspondence leads to some basic characterizations of these codes such as generator and parity check polynomials among others. We are also interested in the algebraic structure of ℓ -quasi-monomial codes of length $n = \ell m$ with associated vector $a = (a_0, a_1, \dots, a_{m-1})$, which are identified by the $R_{q,m}$ -submodules of $R_{q,m}^{\ell}$. In [8] the additive structure of ℓ -quasi-cyclic codes has been investigated, where the authors characterize the $\mathbb{F}_{q^{\ell}}$ -linear images of ℓ -QC codes with respect to a basis of the extension $\mathbb{F}_{q^{\ell}}/\mathbb{F}_q$, and show that such codes must be invariant under certain matrices related to the basis of the extension $\mathbb{F}_{q^{\ell}}/\mathbb{F}_q$. Moreover, when the basis of the extension $\mathbb{F}_{q^{\ell}}/\mathbb{F}_q$ is normal the characterization is particularly simple. Following that paper, we gave a similar characterization for ℓ -QM codes. Finally, we are interested in the asymptotic performance of QM codes, where we follow [1] and [14] to show that ℓ -QM codes and additive monomial codes are asymptotically good.

This paper is organized as follows. We give the necessary background on monomial codes and linear codes invariant under a monomial matrix in section 2. The algebraic structure of ℓ -quasi-monomial codes and their polynomials characterizations are in section 3. Section 4 is devoted to investigating the additive structure of quasi-monomial codes and a characterization of their $\mathbb{F}_{q^{\ell}}$ -linear images with respect to a basis of the extension $\mathbb{F}_{q^{\ell}}/\mathbb{F}_q$. Finally, in section 5, we study the asymptotic performance of QM codes and additive monomial codes.

2. Codes invariant under a monomial matrix

Let us start with the following definition of a monomial code.

Definition 2.1 (Definition 3.1 [4]). *A linear code $C \subseteq \mathbb{F}_q^n$ is called **monomial** code with associated vector $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^{*n}$ if for each codeword $c = (c_0, c_1, \dots, c_{n-1}) \in C$, we have $c' = (a_{n-1}c_{n-1}, a_0c_0, \dots, a_{n-2}c_{n-2})$ is also a codeword.*

Remark 2.2. *From the above definition we observe that monomial codes are invariant under the operator*

$T_{\bar{a}}$, called the monomial shift induced by $a = (a_0, a_1, \dots, a_{n-1})$, defined by:

$$T_{\bar{a}}(v_0, v_1, \dots, v_{n-1}) = (a_{n-1}v_{n-1}, a_0v_0, \dots, a_{n-2}v_{n-2}). \quad (1)$$

We recall now the definition of a monomial matrix.

Definition 2.3 ([5]). 1. An $n \times n$ matrix $M = (M_{ij})_{1 \leq i, j \leq n}$ is called a **monomial** if it is a regular matrix and has in each row and each column exactly one non-zero component.

2. An $n \times n$ matrix $P = (P_{ij})_{1 \leq i, j \leq n}$ called a **permutation matrix** if there is a permutation $\sigma \in S_n$ such that P is obtained by permuting the columns of the identity matrix I_n i.e., $P_{ij} = \begin{cases} 1 & \text{if } i = \sigma(j) \\ 0 & \text{if } i \neq \sigma(j) \end{cases}$, for any $1 \leq i, j \leq n$ and we write $P = P_{\sigma}$.

3. A permutation matrix P_{σ} is a monomial matrix with all non-zero components equal to 1.

Lemma 2.4 ([5], Lemma 2). If M is a monomial matrix of order n with non-zero components $a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_q^*$, then there is a permutation $\sigma \in S_n$ such that $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_{\sigma}$.

Remark 2.5. Observe that monomial codes are invariant under the action of the following monomial matrix

$$A_{\bar{a}} = \text{diag}(a_0, a_1, \dots, a_{n-1})P_{\sigma} = \begin{pmatrix} 0 & 0 & \dots & 0 & a_{n-1} \\ a_0 & 0 & \dots & 0 & 0 \\ 0 & a_1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & a_{n-2} & 0 \end{pmatrix} \quad (2)$$

with σ is the n -cycle defined by $\sigma(1, 2, \dots, n) = (n, 1, \dots, n-1)$. We refer to this n -cycle as a **standard n -cycle** or as an n -cycle of **standard form**.

Let $\lambda = \prod_{i=0}^{n-1} a_i$. It is shown in [4] that there is an invertible matrix Q such that $A_{\lambda} = Q^{-1}A_{\bar{a}}Q$, where

$$A_{\lambda} = \begin{pmatrix} 0 & 0 & \dots & 0 & \prod_{i=0}^{n-1} a_i \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & 1 & \ddots & \vdots & \vdots \\ \vdots & \dots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}, \quad Q = \begin{pmatrix} 0 & 0 & \dots & 0 & \prod_{i=0}^{n-1} a_i \\ a_0 & 0 & \dots & 0 & 0 \\ \vdots & a_0 a_1 & \ddots & \vdots & \vdots \\ \vdots & \dots & \ddots & 0 & \vdots \\ 0 & 0 & \dots & \prod_{i=0}^{n-2} a_i & 0 \end{pmatrix} \quad (3)$$

Proposition 2.6. A linear code $C \subseteq \mathbb{F}_q^n$ is a monomial code with associated vector $a = (a_0, a_1, \dots, a_{n-1})$ if and only if $Q^{-1}C$ is a λ -constacyclic code, where $\lambda = \prod_{i=0}^{n-1} a_i$.

Proof. If C is monomial then $T_{\bar{a}}(C) = A_{\bar{a}}C \subseteq C$. As $A_{\lambda} = Q^{-1}A_{\bar{a}}Q$, we have

$$A_{\lambda}Q^{-1}C = Q^{-1}A_{\bar{a}}QQ^{-1}C = Q^{-1}A_{\bar{a}}C \subseteq Q^{-1}C.$$

It follows that $Q^{-1}C$ is a λ -constacyclic code. $\square$

In the following proposition we present a result about codes invariant under a monomial matrix $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_{\sigma}$, where σ is an n -cycle.

Proposition 2.7. Let $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$, where σ is an n -cycle and $C \subseteq \mathbb{F}_q^n$ be a linear code invariant under M . Then

1. if σ is of standard form, then C is a monomial code with associated vector $a = (a_0, a_1, \dots, a_{n-1})$.
2. if σ is not of standard form, then there is a permutation $\rho \in S_n$, and an invertible matrix $Q_\rho = P_\rho Q$, such that $Q_\rho^{-1}C$ is a monomial code with associated vector $a = (a_0, a_1, \dots, a_{n-1})$.

Proof. 1. From Remark 2.5, M is exactly the monomial matrix $A_{\bar{a}}$.

2. Let $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$ be a monomial matrix and σ' be the n -cycle of standard form as in Remark 2.5. As P_σ and $P_{\sigma'}$ have same minimal polynomial $f(x) = x^n - 1$, one can construct a permutation ρ such that $\sigma' = \rho\sigma\rho^{-1}$ and $P_{\sigma'} = P_\rho^{-1}P_\sigma P_\rho$. Therefore the multiplication by $\text{diag}(a_0, a_1, \dots, a_{n-1})$ both sides leads to $A_{\bar{a}} = P_\rho^{-1}MP_\rho$. Hence by a similar argument as in the proof Proposition 2.6, the result holds. $\square$

From the two propositions above, we deduce the following result.

Corollary 2.8. Let $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$ be a monomial matrix, where σ is an n -cycle, and C is a linear code of length n over $\mathbb{F}_q$. Then C is invariant under M if and if $Q_\rho^{-1}C$ is a $\prod_{i=0}^{n-1} a_i$ -constacyclic code, where $Q_\rho = QP_\rho$, P_ρ is the permutation matrix of ρ , as in Proposition 2.7, and Q is the invertible matrix as in (3).

Proof. Follows from $A_\lambda = Q_\rho^{-1}MQ_\rho$. $\square$

We now present a result about codes invariant under a monomial matrix $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$, where σ is an arbitrary permutation not necessarily an n -cycle. First, recall that any permutation $\sigma \in S_n$ can be written as a product of r disjoint n_i -cycles σ_i where $n = n_1 + n_2 + \dots + n_r$. We have

Proposition 2.9. Let $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$, where $\sigma = \sigma_1\sigma_2\dots\sigma_r$ a product of r disjoint n_i -cycles σ_i , and let $C \subseteq \mathbb{F}_q^n$ be a linear code invariant under M . Then C can be decomposed as

$$C = C_1 \oplus C_2 \oplus \dots \oplus C_r$$

where each C_i is a linear code of length n_i invariant under the monomial matrix $M_i = \text{diag}(a_{i_1}, a_{i_2}, \dots, a_{i_{n_i}})P_{\sigma_i}$, where the support of each σ_i is $\text{supp}(\sigma_i) = \{i_1, i_2, \dots, i_{n_i}\}$. Moreover, if each σ_i is of standard form, then C can be decomposed as a direct sum of monomial codes C_i with associated vector $(a_{i_1}, a_{i_2}, \dots, a_{i_{n_i}}) \in \mathbb{F}_q^{n_i}$.

Proof. Follows from the fact that $\text{diag}(M_1, M_2, \dots, M_r)$ and M are similar matrices. $\square$

Remark 2.10 (Codes invariant under a permutation). With the same notations as in the propositions above, if $a_i = 1$ for all $i = 0, \dots, n-1$, then we obtain cyclic codes and their various generalizations such as quasi-cyclic codes and generalized quasi-cyclic codes.

To use the polynomial ring in the study of monomial codes, let us consider $\varphi_{\bar{a}}$, the $\mathbb{F}_q$ -vector space isomorphism between $\mathbb{F}_q^n$ and $R_{q,n} := \mathbb{F}_q[x]/\langle x^n - \prod_{i=0}^{n-1} a_i \rangle$, defined by :

$$\begin{aligned} \varphi_{\bar{a}} : \quad \mathbb{F}_q^n &\longrightarrow R_{q,n} \\ v = (v_0, v_1, \dots, v_{n-1}) &\longmapsto \varphi_{\bar{a}}(v) = \sum_{i=0}^{n-2} \left(v_{i+1} \prod_{k=0}^i a_k^{-1} \right) x^i + \left(v_0 \prod_{i=0}^{n-1} a_i^{-1} \right) x^{n-1} \end{aligned} \quad (4)$$

Theorem 2.11. A linear code $C \subseteq \mathbb{F}_q^n$ is a monomial code with associated vector $a = (a_0, a_1, \dots, a_{n-1})$ if and only if $\varphi_{\bar{a}}(C)$ is an ideal of $R_{q,n}$. So, a monomial code is a constacyclic code after a monomial permutation.

Proof. Suppose that C is a monomial code and let $c = (c_0, c_1, \dots, c_{n-1}) \in C$. Then

$$\begin{aligned} x\varphi_{\bar{a}}(c) &= x \left(c_1 a_0^{-1} + (a_0 a_1)^{-1} c_2 x + \dots + c_{n-1} \prod_{i=0}^{n-2} a_i^{-1} x^{n-2} + c_0 \prod_{i=0}^{n-1} a_i^{-1} x^{n-1} \right) \\ &= c_1 a_0^{-1} x + (a_0 a_1)^{-1} c_2 x^2 + \dots + c_{n-1} \prod_{i=0}^{n-2} a_i^{-1} x^{n-1} + c_0 \prod_{i=0}^{n-1} a_i^{-1} x^n \\ &= c_0 + (c_1 a_0^{-1}) x + (a_0^{-1} a_1^{-1} c_2) x^2 + \dots + \left(c_{n-1} \prod_{i=0}^{n-2} a_i^{-1} \right) x^{n-1} \left(\text{mod } x^n - \prod_{i=0}^{n-1} a_i \right) \end{aligned} \quad (5)$$

As the inverse of $\varphi_{\bar{a}}^{-1}$ is given by

$$\varphi_{\bar{a}}^{-1}(c_0 + c_1 x + \dots + c_{n-1} x^{n-1}) = \left(c_{n-1} \prod_{i=0}^{n-1} a_i, a_0 c_0, a_0 a_1 c_1, \dots, c_{n-2} \prod_{i=0}^{n-2} a_i \right),$$

we obtain

$$\begin{aligned} \varphi_{\bar{a}}^{-1}(x\varphi_{\bar{a}}(c)) &= \left(c_{n-1} \prod_{i=0}^{n-1} a_i \prod_{i=0}^{n-2} a_i^{-1}, a_0 c_0, a_0 a_1 c_1 a_0^{-1}, \dots, c_{n-2} \prod_{i=0}^{n-2} a_i \prod_{i=0}^{n-3} a_i^{-1} \right) \\ &= (c_{n-1} a_{n-1}, a_0 c_0, a_0 c_1, \dots, c_{n-2} a_{n-2}) \\ &= T_{\bar{a}}(c_0, c_1, \dots, c_{n-1}) \in C, \text{ since } C \text{ is monomial.} \end{aligned} \quad (6)$$

And so,

$$x\varphi_{\bar{a}}(c) \in \varphi_{\bar{a}}(C).$$

By induction we show that for each polynomial $f(x) \in \mathbb{F}_q[x]$, $f(x)\varphi_{\bar{a}}(c) = \varphi_{\bar{a}}(f(A_{\bar{a}})(c))$. Finally $\varphi_{\bar{a}}(C)$ is an ideal of $R_{q,n}$. $\square$

From the above theorem we deduce the following characterization of monomial codes.

Proposition 2.12. Let $C \subseteq \mathbb{F}_q^n$ be a monomial code of length n over $\mathbb{F}_q$.

1. There is a monic polynomial of least degree $g(x) \in \mathbb{F}_q[x]$ such that $g(x)$ divides $f_{\bar{a}}(x) = x^n - \prod_{i=0}^{n-1} a_i$.
and $\varphi_{\bar{a}}(C) = \langle g(x) \rangle$.
2. The set $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$ forms a basis of $\varphi_{\bar{a}}(C)$ and the dimension of C is $k = n - \deg(g)$.
3. A generator matrix G of C is given by:

$$G = \begin{pmatrix} \varphi_{\bar{a}}^{-1}(g(x)) \\ \varphi_{\bar{a}}^{-1}(xg(x)) \\ \vdots \\ \varphi_{\bar{a}}^{-1}(x^{k-1}g(x)) \end{pmatrix} \quad (7)$$

where $k = n - \deg(g)$ and $g(x) = \sum_{i=0}^{n-k} g_i x^i$.

Remark 2.13. Note that the irreducible factorization of $f_{\bar{a}}(x) = x^n - \prod_{i=0}^{n-1} a_i$ over $\mathbb{F}_q$ permits to construct all monomial codes $C \subseteq \mathbb{F}_q^n$ with associated vector $a = (a_0, a_1, \dots, a_{n-1})$.

Let us recall that Euclidean dual of a linear code $C \subseteq \mathbb{F}_q^n$ is defined by

$$C^\perp := \left\{ x \in \mathbb{F}_q^n : \langle x, c \rangle = 0, \forall c \in C \right\}.$$

Theorem 2.14. Let C be a monomial code with associate vector $a = (a_0, a_1, \dots, a_{n-1})$. Then $C^\perp$ is also a monomial code with associate vector $a^{-1} = (a_0^{-1}, a_1^{-1}, \dots, a_{n-1}^{-1})$.

Proof. If C is a monomial code, then by Proposition 2.6, $Q^{-1}C$ is a λ -constacyclic code. It follows that $(Q^{-1}C)^\perp = Q^{-1}C^\perp$ is a λ^{-1} -constacyclic code, i.e.,

$$A_{\lambda^{-1}} Q^{-1} C^\perp \subseteq Q^{-1} C^\perp$$

As $A_{\lambda^{-1}} = Q^{-1} A_{\bar{a}^{-1}} Q$, we have

$$Q^{-1} A_{\bar{a}^{-1}} Q Q^{-1} C^\perp = Q^{-1} A_{\bar{a}^{-1}} C^\perp \subseteq Q^{-1} C^\perp.$$

It follows that $A_{\bar{a}^{-1}} C^\perp \subseteq C^\perp$ which means that $C^\perp$ is a monomial code with associate vector $a^{-1} = (a_0^{-1}, a_1^{-1}, \dots, a_{n-1}^{-1})$. $\square$

From the above proposition, we deduce easily the following result.

Corollary 2.15. Let $M = \text{diag}(a_0, a_1, \dots, a_{n-1}) P_\sigma$ be a monomial matrix, with σ an n -cycle, and C a linear code invariant under M . Then $P_\rho^{-1} C^\perp$ is a monomial code with associate vector $a^{-1} = (a_0^{-1}, a_1^{-1}, \dots, a_{n-1}^{-1})$, where P_ρ is the permutation matrix of $\rho \in S_n$ as in Corollary 2.8.

Proof. Follows from $A_{\bar{a}^{-1}} = P_\rho M P_\rho^{-1}$. $\square$

Example 2.16. Let $a = (1, \alpha, 2, \alpha^2, 4) \in \mathbb{F}_9^5 = \mathbb{F}_3^5(\alpha)$, where α is a root of $f_\alpha(x) = x^2 + 2x + 2$. Let the irreducible factorization of $f_{\bar{a}}(x) = x^5 - (1 \times \alpha \times 2 \times \alpha^2 \times 4) = x^5 - (2\alpha + 1)$ be:

$$f_{\bar{a}}(x) = x^5 - (2\alpha + 1) = (x + 2\alpha + 1) \cdot (x^2 + x + 2\alpha + 2) \cdot (x^2 + (\alpha + 1)x + 2\alpha + 2).$$

Hence, one can construct $2^3 - 2 = 6$ non trivial monomial codes of length 5 over $\mathbb{F}_9$ with associated vector $a = (1, \alpha, 2, \alpha^2, 4)$, with generator polynomials

$$\begin{aligned} g_1 &= x + 2\alpha + 1, \\ g_2 &= x^3 + 2x^2 + (\alpha + 2)x + \alpha, \\ g_3 &= x^3 + (2\alpha + 2)x^2 + \alpha x + \alpha, \\ g_4 &= x^4 + (\alpha + 2)x^3 + (2\alpha + 2)x^2 + 2\alpha x + 2, \\ g_5 &= x^2 + (\alpha + 1)x + 2\alpha + 2, \\ g_6 &= x^2 + x + 2\alpha + 2 \end{aligned}$$

For example, the linear code C such that $\varphi(C) = \langle x^3 + 2x^2 + (\alpha + 2)x + \alpha \rangle$, is a $[5, 2, 4]$ -linear code with a generator matrix

$$G = \begin{pmatrix} \alpha + 2 & 2\alpha + 1 & 2 & 0 & 2\alpha + 2 \\ \alpha & 2\alpha + 2 & 1 & 2\alpha + 2 & 0 \end{pmatrix},$$

which is an MDS code, we can easily check that the Singleton bound is attained here.

3. Monomial codes as invariant subspaces

Following [4, 12, 15] and [13], we can give a characterization of monomial codes by the theory of invariant subspaces. As $f_{\bar{a}}(x) = x^n - \prod_{i=0}^{n-1} a_i$ is the minimal polynomial of $T_{\bar{a}}$, its irreducible factorization allows us to obtain the desired result. So, let

$$f_{\bar{a}}(x) = \prod_{i=1}^r f_i^{\alpha_i}(x) \quad (8)$$

where $f_i(x)$ are irreducible polynomials. By the Cayley-Hamilton theorem [9, Theorem 4 p. 194], the matrix $A_{\bar{a}}$ satisfies

$$f(A_{\bar{a}}) = 0$$

For $i = 1, \dots, r$, let U_i be the null space of each $f_i^{\alpha_i}(x)$, i.e.,

$$U_i := \ker \left(f_i^{\alpha_i}(A_{\bar{a}}) \right) = \left\{ v \in \mathbb{F}_q^n : f_i^{\alpha_i}(A_{\bar{a}}) v = 0 \right\}. \quad (9)$$

For polycyclic codes, the following Lemma has been proved in [12, Theorem 3]. In our case of monomial codes, we omit the proof and state that one can obtain the result by replacing the operator $T_{\bar{a}}$ by T_R , in terms of [12].

Lemma 3.1 ([12], Theorem 3). *The subspaces U_i of $\mathbb{F}_q^n$ satisfy the following conditions :*

1. $\mathbb{F}_q^n = U_1 \oplus U_2 \oplus \dots \oplus U_r$.
2. U_i is an invariant subspace of $\mathbb{F}_q^n$ under $T_{\bar{a}}$
3. If W is an invariant subspace of $\mathbb{F}_q^n$ under $T_{\bar{a}}$ and $W_i = W \cap U_i$, for $i = 1, \dots, r$, then W_i is also invariant under $T_{\bar{a}}$ and $W = W_1 \oplus W_2 \oplus \dots \oplus W_r$.
4. $\varphi_{\bar{a}}(U_i)$ is the ideal of $R_{q,n}$ generated by $\widehat{f_i^{\alpha_i}}(x)$, where $\widehat{f_i^{\alpha_i}}(x) = \frac{f_{\bar{a}}(x)}{f_i^{\alpha_i}(x)}$.
5. The dimension of U_i is given by $\dim_{\mathbb{F}_q}(U_i) = \deg(f_i^{\alpha_i}) = \alpha_i \deg(f_i)$.
6. If $P(x)$ is a divisor of $f_{\bar{a}}(x)$ in $\mathbb{F}_q[x]$, then $\ker(P(A_{\bar{a}}))$ is a direct sum of invariant subspaces of $\mathbb{F}_q^n$.
7. If $\gcd(n, p) = 1$, then U_i is a minimal invariant subspace of $\mathbb{F}_q^n$ under $T_{\bar{a}}$
8. If $\gcd(n, p) = 1$ and $P(x)$ is a divisor of $f_{\bar{a}}(x)$ in $\mathbb{F}_q[x]$, then $\ker(P(A_{\bar{a}}))$ is a direct sum of minimal invariant subspaces of $\mathbb{F}_q^n$.

From the above Lemma and Proposition 2.12 we have the following characterization of the monomial codes.

Theorem 3.2. *Let C be a monomial code of length n over $\mathbb{F}_q$ generated by $g(x) = \prod_{i=1}^r f_i^{k_i}(x)$, $0 \leq k_i \leq \alpha_i$ and $h(x) \in \mathbb{F}_q[x]$ such that $f_{\bar{a}}(x) = h(x)g(x)$. Then*

1. $\varphi_{\bar{a}}(C) = \varphi_{\bar{a}}(\ker(h(T_{\bar{a}})))$

2. $C = \ker(h(T_{\bar{a}}))$ and $\dim_{\mathbb{F}_q}(C) = \text{rank}(h(T_{\bar{a}})) = \deg(g)$.
3. $C = C_1 \oplus C_2 \oplus \cdots \oplus C_r$ where C_i is the monomial code generated by $g_i(x) = \text{lcm}(g(x), \widehat{f_i^{\alpha_i}}(x)) = f_i^{k_i}(x) \widehat{f_i^{\alpha_i}}(x)$, for all $i = 1, \dots, r$.
4. If $\gcd(n, p) = 1$, then $C = C_1 \oplus C_2 \oplus \cdots \oplus C_r$, where C_i is a minimal monomial code.

Proof. 1. Let $c(x) = \sum_{i=0}^{n-1} c_i x^i \in \varphi_{\bar{a}}(C)$. Since $\varphi_{\bar{a}}(C) = \langle g(x) \rangle$, there is $a(x) \in \mathbb{F}_q[x]$ such that $c(x) = a(x)g(x)$. It follows that

$$h(x)c(x) = h(x)a(x)g(x) = 0 \text{ mod } f_{\bar{a}}(x).$$

So

$$h(x)c(x) = \sum_{i=0}^{\deg(h)} h_i x^i c(x) = \sum_{i=0}^{\deg(h)} h_i \varphi_{\bar{a}}(T_{\bar{a}}^i(c)) = \varphi_{\bar{a}}\left(\sum_{i=0}^{\deg(h)} h_i T_{\bar{a}}^i(c)\right) = \varphi_{\bar{a}}(h(T_{\bar{a}})(c))$$

Hence, $h(T_{\bar{a}})(c) = 0$, which means that $c \in \ker(h(T_{\bar{a}}))$ and $\varphi_{\bar{a}}(C) \subseteq \varphi_{\bar{a}}(\ker(h(T_{\bar{a}})))$. Conversely, let $a(x) \in \varphi_{\bar{a}}(\ker(h(T_{\bar{a}})))$. There exist $q(x), r(x) \in \mathbb{F}_q[x]$ such that

$$a(x) = q(x)g(x) + r(x) \text{ where } \deg(r(x)) < \deg(g(x)).$$

Then $h(x)r(x) = 0 \text{ mod } f_{\bar{a}}(x)$.

Assume that $r(x) \neq 0$. Let $K(x) \in \mathbb{F}_q[x]$ such that $h(x)r(x) = K(x)f_{\bar{a}}(x)$. Since $f_{\bar{a}}(x)$ is monic,

$$\deg(h(x)r(x)) = \deg(K(x)f_{\bar{a}}(x)) = \deg(K(x)) + \deg(f_{\bar{a}}(x)) \geq n.$$

Otherwise, as $h(x)$ is monic we have

$$\deg(h(x)r(x)) = \deg(h) + \deg(r(x)) < n$$

Contradiction. Hence $r(x) = 0$ and $a(x) \in \varphi_{\bar{a}}(C)$.

2. The result follows from the statement above.

3. Let $C_i = C \cap U_i$, for all $i = 1, \dots, r$. The monomial code C_i is generated by

$$g_i(x) = \text{lcm}(g(x), \widehat{f_i^{\alpha_i}}(x)) = f_i^{k_i}(x) \widehat{f_i^{\alpha_i}}(x)$$

By the statement 3 of Lemma 3.1, we have that $C = C_1 \oplus C_2 \oplus \cdots \oplus C_r$.

4. Follows immediately from the statement above.

□

4. Quasi-monomial codes

Definition 4.1 (Quasi-monomial code). Let $n = m\ell$ and $a = (a_0, a_1, \dots, a_{m-1}) \in \mathbb{F}_q^m$. A linear code $C \subseteq \mathbb{F}_q^n$ is called ℓ -**quasi-monomial** of index ℓ over $\mathbb{F}_q$, if and only if for each codeword

$$c = \left(\overbrace{c_{0,0}, c_{0,1}, \dots, c_{0,\ell-1}}^{c_0}, \overbrace{c_{1,0}, c_{1,1}, \dots, c_{1,\ell-1}}^{c_1}, \dots, \overbrace{c_{m-1,0}, c_{m-1,1}, \dots, c_{m-1,\ell-1}}^{c_{m-1}} \right) \in C,$$

ℓ is the smallest integer such that $c_{\bar{a}} = (a_{m-1}c_{m-1}, a_0c_0, \dots, a_{m-2}c_{m-2}) \in C$.

Remark 4.2. Observe that each ℓ -quasi-monomial code C of length $n = m\ell$, over $\mathbb{F}_q$ can be viewed as a monomial code of length m over $\mathbb{F}_{q^\ell}$.

Let $\tilde{a} = (a_0, a_1, \dots, a_{m-1}) \in \mathbb{F}_q^m$, and define the ℓ -quasi-monomial shift $\psi_{\tilde{a}}$ by:

$$\begin{aligned} \psi_{\tilde{a}} : \quad \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^n \\ v = (v_0, v_1, \dots, v_{n-1}) &\longmapsto \psi_{\tilde{a}}(v) = A_{\tilde{a}}(v_0, v_1, \dots, v_{n-1})^t \end{aligned}$$

where

$$A_{\tilde{a}} = \begin{pmatrix} 0 & \dots & 0 & A_{a_{m-1}} \\ A_{a_0} & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & A_{a_{m-2}} & 0 \end{pmatrix}_{m\ell \times m\ell} \quad (10)$$

and each $A_{a_i} = \text{diag}(\overbrace{a_i, \dots, a_i}^{\ell \text{ times}})$, is the $\ell \times \ell$ square matrix with a_i on the position (j, j) and 0 elsewhere.

Proposition 4.3. A linear code $C \subseteq \mathbb{F}_q^n$ is an ℓ -quasi-monomial code of length $n = m\ell$ if and only if it is invariant under $\psi_{\tilde{a}}$.

Let $I_{\tilde{a}}$ be the principal ideal of $\mathbb{F}_q[x]$ generated by $f_{\tilde{a}}(x) = x^m - \prod_{i=0}^{m-1} a_i$. As $f_{\tilde{a}}(x)$ is the minimal polynomial of $\psi_{\tilde{a}}$, $I_{\tilde{a}} \cdot \mathbb{F}_q^{m\ell} = \{0\}$, the operator $\psi_{\tilde{a}}$ equips $\mathbb{F}_q^{m\ell}$ with an $R_{q,m}$ -module structure where the multiplication is given by:

$$\begin{aligned} R_{q,m} \times \mathbb{F}_q^{m\ell} &\longrightarrow \mathbb{F}_q^{m\ell} \\ (P, v) &\longmapsto P.v := P(\psi_{\tilde{a}})(v). \end{aligned} \quad (11)$$

Let us define the following $R_{q,m}$ -module isomorphism $\varphi_{\tilde{a}, \ell}$ by:

$$\begin{aligned} \varphi_{\tilde{a}, \ell} : \quad \mathbb{F}_q^{m\ell} &\longrightarrow R_{q,m}^\ell \\ (c_0, c_1, \dots, c_{m-1}) &\longmapsto (\tilde{c}_0(x), \tilde{c}_1(x), \dots, \tilde{c}_{\ell-1}(x)) \end{aligned} \quad (12)$$

where for $0 \leq k \leq \ell - 1$,

$$\tilde{c}_k(x) = \varphi_{\tilde{a}}(c_{0,k}, c_{1,k}, \dots, c_{m-1,k}) = \sum_{i=0}^{m-2} \left(c_{i+1,k} \prod_{k=0}^i a_k^{-1} \right) x^i + \left(c_{0,k} \prod_{i=0}^{m-1} a_i^{-1} \right) x^{n-1}.$$

Thus we deduce the following result.

Theorem 4.4. A linear code $C \subseteq \mathbb{F}_q^{m\ell}$, is an ℓ -QM code with associated vector $a = (a_0, a_1, \dots, a_{m-1})$ if and only if $\varphi_{\tilde{a}, \ell}(C)$ is an $R_{q,m}$ -submodule of $R_{q,m}^\ell$.

Definition 4.5 (r -generator quasi-monomial code). An ℓ -QM code $C \subseteq \mathbb{F}_q^{m\ell}$ is called a r -generator ℓ -QM code if $\varphi_{\tilde{a}, \ell}(C)$ is generated by r elements as an $R_{q,m}$ -submodule of $R_{q,m}^\ell$, i.e., there exist $\underline{a}_1(x), \underline{a}_2(x), \dots, \underline{a}_r(x)$ in $R_{q,m}^\ell$ such that

$$\varphi_{\tilde{a}, \ell}(C) = R_{q,m} \underline{a}_1(x) + R_{q,m} \underline{a}_2(x) + \dots + R_{q,m} \underline{a}_r(x).$$

We close this section by the following characterization of an r -generator quasi-monomial code.

Proposition 4.6. *Let $C \subseteq \mathbb{F}_q^{mr}$ be an r -generator right quasi-monomial code generated by $\underline{a}_1(x), \underline{a}_2(x), \dots, \underline{a}_s(x)$ where $\underline{a}_i(x) = (a_{i,0}(x), a_{i,1}(x), \dots, a_{i,\ell-1}(x))$ for $1 \leq i \leq r$. Then, there exist $b_{i,j}(x)$, $1 \leq j \leq r$, $0 \leq j \leq \ell-1$, such that $a_{i,j}(x) = b_{i,j}(x)g_j(x)$ where $g_{i,j}(x)$ divides $f_{\bar{a}}(x)$.*

Proof. As C is an r -generator quasi-monomial code, we have

$$\varphi_{\bar{a},\ell}(C) = R_{q,m}\underline{a}_1(x) + R_{q,m}\underline{a}_2(x) + \dots + R_{q,m}\underline{a}_r(x)$$

for some $\underline{a}_i(x) = (a_{i,0}(x), a_{i,1}(x), \dots, a_{i,\ell-1}(x)) \in R_{q,m}^r$, $1 \leq i \leq r$. As each $R_{q,m}\underline{a}_i(x)$, $i = 1, \dots, r$, is a 1-generator quasi-monomial code, then

$$R_{q,m}\underline{a}_i(x) = R_{q,m}a_{i,0}(x) \oplus R_{q,m}a_{i,1}(x) \oplus \dots \oplus R_{q,m}a_{i,\ell-1}(x),$$

where $R_{q,m}a_{i,j}(x)$, $j = 0, \dots, \ell-1$ is a monomial code of length m . Let $g_{i,j}(x)$ be its generator polynomial. Then there exists $b_{i,j}(x) \in R_{q,m}$ such that $a_{i,j}(x) = b_{i,j}(x)g_{i,j}(x)$. $\square$

An important class of quasi-monomial codes is the 1-generator quasi-monomial codes, as we can define the generator polynomial, the parity check polynomial, and then compute the dimension of each 1-generator quasi-monomial code. Let us recall that C is a 1-generator ℓ -QM code if it is generated by one element $\underline{a}(x) = (a_0(x), a_1(x), \dots, a_{\ell-1}(x)) \in R_{q,m}^\ell$, (i.e)

$$\varphi_{\bar{a},\ell}(C) = R_{q,m} \cdot \underline{a}(x) = R_{q,m}(a_0(x), a_1(x), \dots, a_{\ell-1}(x)) \subseteq R_{q,m}^\ell.$$

Definition 4.7. *Let C be a 1-generator quasi-monomial code generated by $\underline{a}(x) = (a_1(x), a_2(x), \dots, a_r(x))$. The polynomial*

1. $g(x) = \gcd(\underline{a}(x), f_{\bar{a}}(x))$ is called the **generator polynomial** (g.p.) of C .
2. $h(x) = \frac{f_{\bar{a}}(x)}{g(x)}$ is called the **parity check polynomial** (p.c.p.) of C .

From Proposition 2.12, we easily deduce the following characterisation of 1-generator quasi-monomial codes.

Proposition 4.8. *Let C be a 1-generator quasi-monomial code generated by $\underline{a}(x) = (a_0(x), a_1(x), \dots, a_{\ell-1}(x)) \in R_{q,m}^\ell$ with $g(x)$, $h(x)$ as g.p and p.c.p. respectively, $g_i(x) = \gcd(a_i(x), f_{\bar{a}}(x))$, $i = 0, \dots, \ell-1$, and $\underline{g}(x) = (g_0(x), g_1(x), \dots, g_{\ell-1}(x))$. Then,*

1. C has a generator of the form

$$(p_0(x)g_0(x), p_1(x)g_1(x), \dots, p_{\ell-1}(x)g_{\ell-1}(x))$$

where $\gcd(p_i, h) = 1$.

2. $g(x) = \gcd(g_1(x), g_2(x), \dots, g_r(x))$ and $h(x) = \text{lcm}\{h_i(x) : 1 \leq i \leq r\}$.
3. $\dim_{\mathbb{F}_q}(C) = \deg(h(x))$, and

$$S = \{(x^i g_1(x), x^i g_2(x), \dots, x^i g_r(x)) : 0 \leq i \leq \deg(h(x)) - 1\}$$

forms a basis of C .

4. a generator matrix of C is given by

$$G = \begin{pmatrix} \underline{g}(x) \\ x\underline{g}(x) \\ \vdots \\ x^{k-1}\underline{g}(x) \end{pmatrix} = \begin{pmatrix} g_0(x) & g_1(x) & \dots & g_{\ell-1}(x) \\ xg_0(x) & xg_1(x) & \dots & xg_{\ell-1}(x) \\ \vdots & \vdots & \vdots & \vdots \\ x^{k-1}g_0(x) & x^{k-1}g_1(x) & \dots & x^{k-1}g_{\ell-1}(x) \end{pmatrix} \quad (13)$$

where $k = \deg(h(x))$.

Assume that $\gcd(m, q) = 1$ and let the irreducible factorization of $f_{\bar{a}} = x^m - \prod_{i=0}^{m-1} a_i$ be

$$f_{\bar{a}}(x) = x^m - \prod_{i=0}^{m-1} a_i = f_1(x)f_2(x) \dots f_s(x)$$

By the Chinese Remainder Theorem (CRT) we have the following ring isomorphism:

$$R_{q,m} \cong \bigoplus_{i=1}^s \mathbb{F}_q[x] / \langle f_i(x) \rangle$$

Let β be a primitive m^{th} root of unity and $\beta^m = \prod_{i=0}^{n-1} a_i$. Then the roots of $f_{\bar{a}}$ are $\beta\xi^i$, $i = 0, \dots, m-1$.

As each $f_i(x), i = 0, \dots, n-1$ is irreducible, $\mathbb{E}_i := \mathbb{F}_q(\beta\xi^{u_i})$ is a field, where u_i is the smallest integer such that $\beta\xi^{u_i}$ is a root of $f_i(x)$. Hence $R_{q,m}^{\ell}$ can be decomposed as follows

$$R_{q,m}^{\ell} \cong \mathbb{E}_1^{\ell} \oplus \mathbb{E}_2^{\ell} \oplus \dots \oplus \mathbb{E}_s^{\ell}.$$

So, each ℓ -QM code $\varphi_{\bar{a},\ell}(C)$ can be viewed as an $(\mathbb{E}_1 \oplus \dots \oplus \mathbb{E}_s)$ -submodule of $\mathbb{E}_1^{\ell} \oplus \dots \oplus \mathbb{E}_s^{\ell}$ and can be decomposed as

$$\varphi_{\bar{a},\ell}(C) = C_1 \oplus \dots \oplus C_s \quad (14)$$

where each C_i is a linear code of length ℓ over $\mathbb{E}_i$, and called a **constituent of C** .

As in [8] one can establish that each C_i , $1 \leq i \leq s$ is of the form

$$C_i := \text{Span}_{\mathbb{E}_i} \{(\tilde{c}_0(\xi^{u_i}), \dots, \tilde{c}_{\ell-1}(\xi^{u_i}))\}$$

for each $c(x) = (\tilde{c}_0(x), \dots, \tilde{c}_{\ell-1}(x)) \in \varphi_{\bar{a},\ell}(C)$.

Example 4.9. In this example we are interested in 3-QM codes of length 15 over $\mathbb{F}_9$, with associated vector $a = (1, \alpha, 2, \alpha^2, 4) \in \mathbb{F}_9^5$. As in Example 2.16, let

$$f_{\bar{a}}(x) = x^5 - (2\alpha + 1) = (x + 2\alpha + 1) \cdot (x^2 + x + 2\alpha + 2) \cdot (x^2 + (\alpha + 1)x + 2\alpha + 2).$$

Consider the linear code $C \subseteq \mathbb{F}_9^{15}$ such that $\varphi_{\bar{a},3}(C) = R_{9,5}\underline{a}(x) = R_{9,5}(a_1(x), a_2(x), a_3(x))$, where

$$\begin{aligned} a_1(x) &= \alpha x^4 + (2\alpha + 1)x^2 + (\alpha + 2)x + \alpha + 1 \\ a_2(x) &= (2\alpha + 2)x^4 + (\alpha + 2)x^3 + (2\alpha + 1)x^2 + 2\alpha x + \alpha + 1 \\ a_3(x) &= (2\alpha + 1)x^3 + \alpha x^2 + 2x + 2 \end{aligned}$$

This is a 1-generator 3-QM code with generator $g(x) = \gcd(a_1(x), a_2(x), a_3(x), f_{\bar{a}}(x)) = x + 2\alpha + 1$, and parity check polynomial $h(x) = \frac{f_{\bar{a}}(x)}{g(x)} = x^4 + (\alpha + 2)x^3 + (2\alpha + 2)x^2 + 2\alpha x + 2$. It follows that $\dim_{\mathbb{F}_9}(C) = 4$.

Let $\underline{b}(x) = (b_1(x), b_2(x), b_3(x)) \in R_{9,5}^3$, with

$$\begin{aligned} b_1(x) &= x^3 + (\alpha + 2)x^2 + 2\alpha + 2 \\ b_2(x) &= x^2 + (\alpha + 1)x + 2\alpha + 2 \\ b_3(x) &= (2\alpha + 1)x^3 + (\alpha + 2)x^2 + (\alpha + 1)x + 2 \end{aligned}$$

Then the linear code $C' \subseteq \mathbb{F}_9^{15}$ such that $\varphi_{\underline{a}}(C') = R_{9,5}\underline{a}(x) + R_{9,5}\underline{b}(x)$, is a 2-generator 3-QM code of dimension

$$\dim_{\mathbb{F}_9}(C') = \dim_{\mathbb{F}_9}(R_{9,5}\underline{a}(x)) + \dim_{\mathbb{F}_9}(R_{9,5}\underline{b}(x)) - \dim_{\mathbb{F}_9}(R_{9,5}\underline{a}(x) \cap R_{9,5}\underline{b}(x)) = 4 + 3 - 0 = 7$$

5. Additive structure of monomial codes

Let us start this section with the definitions of additive code and additive monomial code.

Definition 5.1. Let $C \subseteq \mathbb{F}_{q^\ell}^m$ be a subset of $\mathbb{F}_{q^\ell}^m$, where ℓ is a positive integer. Then C is called an **additive** code of length m over $\mathbb{F}_{q^\ell}$ if C is an $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^\ell}^m$.

Definition 5.2. An additive code $C \subseteq \mathbb{F}_{q^\ell}^m$ is called an **additive monomial** code with associated vector $a = (a_0, a_1, \dots, a_{m-1})$ if for each codeword $c = (c_0, c_1, \dots, c_{m-1}) \in C$, we have $c' = (a_{m-1}c_{m-1}, a_0c_0, \dots, a_{m-2}c_{m-2})$ is again a codeword.

Remark 5.3. As in Remark 4.2 we observe that each **additive monomial** code C of length m , over $\mathbb{F}_{q^\ell}$ can be viewed as a monomial code of length m over $\mathbb{F}_{q^\ell}$.

Let $\lambda \in \mathbb{F}_q^*$, a subset $C \subseteq \mathbb{F}_{q^\ell}^m$ is called an additive λ -constacyclic code of length m over $\mathbb{F}_{q^\ell}$ if for each $c = (c_0, c_1, \dots, c_{m-1}) \in C$ we have $c' = (\lambda c_{m-1}, c_0, \dots, c_{m-2}) \in C$.

Proposition 5.4. A linear code $C \subseteq \mathbb{F}_{q^\ell}^n$ is a monomial code with associated vector $a = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{F}_q^n$ if and only if $Q^{-1}C$ is a λ -constacyclic code where $\lambda = \prod_{i=0}^{n-1} a_i$, and Q is the $n \times n$ matrix as in (3).

Proof. The proof is similar to the proof of Proposition 2.6. □

The following map φ is an $R_{q,m}$ -module isomorphism between $\mathbb{F}_{q^\ell}^m$ and $R_{q^\ell,m} := \mathbb{F}_{q^\ell}[x]/\langle x^m - \prod_{i=0}^{m-1} a_i \rangle$.

$$\begin{aligned} \varphi : \quad \mathbb{F}_{q^\ell}^m &\longrightarrow R_{q^\ell,m} \\ v = (v_0, v_1, \dots, v_{m-1}) &\longmapsto \varphi(v) = \sum_{i=0}^{m-2} \left(v_{i+1} \prod_{k=0}^i a_k^{-1} \right) x^i + \left(v_0 \prod_{i=0}^{m-1} a_i^{-1} \right) x^{m-1} \end{aligned} \quad (15)$$

Theorem 5.5. An additive code $C \subseteq \mathbb{F}_{q^\ell}^n$ is a **monomial** code with associated vector $a = (a_0, a_1, \dots, a_{n-1})$ if and only if $\varphi(C)$ is an $R_{q,m}$ -submodule of $R_{q^\ell,m}$.

Proof. Similar to the proof of Theorem 2.11. □

Let $B = \{e_0, \dots, e_{\ell-1}\}$ be a basis of the extension $\mathbb{F}_{q^\ell}/\mathbb{F}_q$. Let us define the following $R_{q,m}$ -module isomorphism between $R_{q,m}^\ell$ and $R_{q^\ell,m}$, by:

$$\begin{aligned} \Phi_B : R_{q,m}^\ell &\longrightarrow R_{\bar{a},q^\ell} \\ c(x) = (\tilde{c}_0(x), \tilde{c}_1(x), \dots, \tilde{c}_{\ell-1}(x)) &\longmapsto \Phi_B(c(x)) = \sum_{i=0}^{\ell-1} \tilde{c}_i(x) e_i. \end{aligned} \quad (16)$$

where $\tilde{c}_k(x) = \sum_{i=0}^{m-2} \left(c_{i+1,k} \prod_{k=0}^i a_k^{-1} \right) x^i + \left(c_{0,k} \prod_{i=0}^{m-1} a_i^{-1} \right) x^{n-1}$, for $k = 0, \dots, \ell - 1$.

Thus Φ_B gives a correspondence between ℓ -quasi-monomial codes of length $n = m\ell$ over $\mathbb{F}_q$, and monomial codes of length m over $\mathbb{F}_{q^\ell}$ (additive monomial codes with associated vector $a = (a_0, a_1, \dots, a_{m-1})$). The proof of the following result is omitted, as it is similar to the case of quasi-cyclic codes.

Proposition 5.6. *A linear code $C \subseteq \mathbb{F}_q^{m\ell}$ is an ℓ -quasi-monomial code with associated $a = (a_0, a_1, \dots, a_{m-1})$, if and only if $\Phi_B(C)$ is an additive monomial code of length m over $\mathbb{F}_{q^\ell}$.*

Now, we ask when the image $\Phi_B(C)$ is a monomial code (not just additive monomial) of length m over $\mathbb{F}_{q^\ell}$. To answer this question, let us consider for each $0 \leq i, j \leq \ell - 1$,

$$e_i e_j = \sum_{k=0}^{\ell-1} \lambda_k^{i,j} e_k \in \mathbb{F}_{q^\ell},$$

and define the $\ell \times \ell$ matrices $M_i, 0 \leq i \leq \ell - 1$ by

$$M_i = \begin{pmatrix} \lambda_0^{i,0} & \lambda_0^{i,1} & \dots & \lambda_0^{i,\ell-1} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{\ell-1}^{i,0} & \lambda_{\ell-1}^{i,1} & \dots & \lambda_{\ell-1}^{i,\ell-1} \end{pmatrix} \quad (17)$$

Following [7], we can prove the following result for ℓ -QM codes.

Theorem 5.7. *Let C be a ℓ -quasi-monomial code of length $n = m\ell$, and let $\varphi_{\bar{a},\ell}(C) = C_1 \oplus C_2 \oplus \dots \oplus C_s$ be its constituent decomposition as in (14). Then,*

$$\begin{aligned} \Phi_B(C) \text{ is } \mathbb{F}_{q^\ell}\text{-linear} &\iff \varphi_{\bar{a},\ell}(C) \text{ is invariant under the matrices } M_i, \ 0 \leq i \leq \ell - 1. \\ &\iff C_i \subseteq \mathbb{E}_i^\ell, \ i = 1, \dots, s \text{ is invariant under the matrices } M_i, \ 0 \leq i \leq \ell - 1. \end{aligned}$$

Proof. Let $c = (c_0, c_1, \dots, c_{m-1}) \in C$, and $c(x) := (\tilde{c}_0(x), \tilde{c}_1(x), \dots, \tilde{c}_{\ell-1}(x)) \in \varphi_{\bar{a},\ell}(C)$. Then

$$\begin{aligned} e_i \Phi_B(c(x)) &= e_i \sum_{j=0}^{\ell-1} \tilde{c}_j(x) e_j. \\ &= \sum_{j=0}^{\ell-1} \tilde{c}_j(x) e_i e_j. \\ &= \sum_{j=0}^{\ell-1} \tilde{c}_j(x) \sum_{k=0}^{\ell-1} \lambda_k^{i,j} e_k \\ &= \tilde{c}_0(x) \left(\lambda_0^{i,0} e_0 + \dots + \lambda_{\ell-1}^{i,0} e_{\ell-1} \right) + \dots + \tilde{c}_{\ell-1}(x) \left(\lambda_0^{i,\ell-1} e_0 + \dots + \lambda_{\ell-1}^{i,\ell-1} e_{\ell-1} \right) \\ &= \left(\lambda_0^{i,0} \tilde{c}_0(x) + \dots + \lambda_0^{i,\ell-1} \tilde{c}_{\ell-1}(x) \right) e_0 + \dots + \left(\lambda_{\ell-1}^{i,0} \tilde{c}_0(x) + \dots + \lambda_{\ell-1}^{i,\ell-1} \tilde{c}_{\ell-1}(x) \right) e_{\ell-1} \end{aligned}$$

$$\begin{aligned}
\Phi_B(C) \text{ is } \mathbb{F}_{q^\ell}\text{-linear} &\iff \forall i = 0, \dots, \ell - 1, \quad e_i \Phi_B(c(x)) \in \Phi_B(C) \\
&\iff \forall i = 0, \dots, \ell - 1, \quad \forall 0 \leq j \leq \ell - 1, \quad \left(\lambda_j^{i,0} \tilde{c}_0(x), \dots, \lambda_j^{i,\ell-1} \tilde{c}_{\ell-1}(x) \right) \in \varphi_{\bar{a},\ell}(C) \\
&\iff \forall i = 0, \dots, \ell - 1, \quad M_i c(x)^t \in \varphi_{\bar{a},\ell}(C)
\end{aligned}$$

This means that $\varphi_{\bar{a}}(C)$ is invariant under multiplication by the matrix M_i , $0 \leq i \leq \ell - 1$. $\square$

Remark 5.8. Suppose that $B = \{1, \alpha, \alpha^2, \dots, \alpha^{\ell-1}\}$ is a basis of the extension $\mathbb{F}_{q^\ell} = \mathbb{F}_q(\alpha)$, and $f_\alpha(x) = x^\ell + \alpha_{\ell-1}x^{\ell-1} + \dots + \alpha_0 \in \mathbb{F}_q[x]$ be the minimal polynomial of α , then following assertions hold.

1. The matrix M_0 in the above theorem is the identity matrix, and each M_i is the matrix corresponding to the multiplication by α^i , for $i = 1, \dots, \ell - 1$.
2. The matrix M_1 is the companion matrix C_{f_α} of the polynomial $f_\alpha(x)$.

From the above remark, we deduce the following characterization of the $\mathbb{F}_{q^\ell}$ –linearity of $\Phi_B(C)$.

Corollary 5.9. Let C be an ℓ –QM code of length $n = m\ell$, and let $\varphi_{\bar{a},\ell}(C) = C_1 \oplus C_2 \oplus \dots \oplus C_s$ be its constituent decomposition as in (14). Then the following statements are equivalent.

1. $\Phi_B(C)$ is $\mathbb{F}_{q^\ell}$ –linear
2. $\varphi_{\bar{a},\ell}(C)$ is invariant under the matrix $M_1 = C_{f_\alpha}$.
3. Each $C_i \subseteq \mathbb{E}_i^\ell$, $i = 1, \dots, s$ is invariant under the matrix C_{f_α} .
4. $C_i \subseteq \mathbb{E}_i^\ell$, is a right polycyclic code of length ℓ over $\mathbb{E}_i$ with associated vector $r = (-\alpha_0, -\alpha_1, \dots, -\alpha_{\ell-1}) \in \mathbb{E}_i^\ell$.
5. There is a monic divisor $g(x)$ of $f_\alpha(x)$ such that $C_i = \langle g(x) \rangle$ is an ideal of $\mathbb{E}_i[x]/\langle f_\alpha(x) \rangle$ and $\dim_{\mathbb{E}_i} = \deg(g(x))$.

Assume that $\gcd(m, q) = 1$ and let $t_i = [\mathbb{E}_i : \mathbb{F}_q]$ be the degree of the extension $\mathbb{E}_i/\mathbb{F}_q$, $b_i = \gcd(\ell, t_i)$, and $d_i = \frac{\ell}{b_i}$. According to [11, Theorem 3.46], the irreducible factorization of $f_\alpha(x)$ over each $\mathbb{E}_i$ is

$$f_\alpha(x) = f_{i,1}(x)f_{i,2}(x) \cdots f_{i,b_i}(x),$$

where each $f_{i,j}(x) \in \mathbb{E}_i[x]$, $j = 1 \dots, b_i$, is of degree d_i .

As in section 3, let for $i = 1, \dots, s$, $j = 1, \dots, b_i$ the null space $U_{i,j}$ of each $f_{i,j}(x)(C_{f_\alpha})$, where C_{f_α} is the companion matrix of f_α which is viewed as an $\ell \times \ell$ matrix in $\mathbb{M}_\ell(\mathbb{E}_i)$, given by

$$U_{i,j} := \ker(f_{i,j}(C_{f_\alpha})) = \{v \in \mathbb{E}_i^\ell : f_{i,j}(C_{f_\alpha})v = 0, j = 0, \dots, b_i\}. \quad (18)$$

Then we have

- $\mathbb{E}_i^\ell = U_{i,1} \oplus U_{i,2} \oplus \dots \oplus U_{i,b_i}$,
- Each $U_{i,j}$, $j = 1, \dots, b_i$ is a minimal invariant subspace of $\mathbb{E}_i^\ell$ under C_{f_α} .
- If W_i is an invariant subspace of $\mathbb{E}_i^\ell$ under C_{f_α} and $W_{i,j} = W_i \cap U_{i,j}$, for $j = 1, \dots, b_i$, then $W_{i,j}$ is also invariant under C_{f_α} and $W_i = W_{i,1} \oplus W_{i,2} \oplus \dots \oplus W_{i,b_i}$.
- $\dim_{\mathbb{E}_i}(U_{i,j}) = \deg(f_{i,j}(x))$. Hence we deduce the following result on the $\mathbb{F}_{q^\ell}$ –linearity of $\Phi_B(C)$ when $\gcd(m, q) = 1$.

Theorem 5.10. Let C be an ℓ -QM code of length $n = m\ell$ over $\mathbb{F}_q$ such that $\Phi_B(C)$ is $\mathbb{F}_{q^\ell}$ -linear, and

$$\varphi_{\bar{\alpha}, \ell}(C) = C_1 \oplus C_2 \oplus \cdots \oplus C_s \subseteq \mathbb{E}_1^\ell \oplus \mathbb{E}_2^\ell \oplus \cdots \oplus \mathbb{E}_s^\ell,$$

be the (constituent) decomposition of C . Then,

1. if $\gcd(\ell, t_i) = 1$, then C_i is either $\{0\}$ or the full space $\mathbb{E}_i^\ell$.
2. otherwise, $\dim_{\mathbb{E}_i}(C_i) = k_i d_i$ for some $0 \leq k_i \leq b_i$.

Proof. If $\Phi_B(C)$ is $\mathbb{F}_{q^\ell}$ -linear, then each $C_i \subseteq \mathbb{E}_i^\ell$ is invariant under C_{f_α} . It follows that

$$C_i = C_i \cap \mathbb{E}_i^\ell = C_{i,1} \oplus C_{i,2} \oplus \cdots \oplus C_{i,b_i}, \quad \text{where each } C_{i,j} := C_i \cap U_{i,j} \text{ as in (18).}$$

1. If $\gcd(\ell, t_i) = 1$, then $f_\alpha(x)$ is irreducible in $\mathbb{E}_i[x]$, and so there is no trivial subspace of $\mathbb{E}_i^\ell$ which is invariant under C_{f_α} . Thus C_i is either $\{0\}$ or the full space $\mathbb{E}_i^\ell$.
2. Otherwise, since each $U_{i,j}$ is a minimal invariant subspace, then as in Corollary 5.9 we see that

$$\dim_{\mathbb{E}_i}(C_{i,j}) = \dim_{\mathbb{E}_i}(C_i \cap U_{i,j}) = \begin{cases} 0 & \text{if } C_i \cap U_{i,j} = \{0\} \\ \deg(f_{i,j}) = d_i & \text{if } C_i \cap U_{i,j} \neq \{0\} \end{cases}$$

$$\text{It follows that } \dim_{\mathbb{E}_i}(C_i) = \sum_{j=1}^{b_i} \dim_{\mathbb{E}_i}(C_{i,j}) = k_i d_i \text{ for some } 0 \leq k_i \leq b_i.$$

□

Corollary 5.11. Let C be a 1-generator ℓ -QM code generated by $\underline{a}(x) = (a_0(x), a_1(x), \dots, a_{\ell-1}(x)) \in R_{q,m}^\ell$, and $g(x)$ be its generator polynomial. If $\Phi_B(C)$ is $\mathbb{F}_{q^\ell}$ -linear then for each $i = 1, \dots, s$ such that $\gcd(\ell, t_i) = 1$, the corresponding constituent $C_i = \{0\}$. This is equivalent to saying that the irreducible factor $f_i(x)$ of $f_{\bar{\alpha}}(x)$ corresponding to $\mathbb{E}_i := \mathbb{F}_q(\beta \xi^{u_i})$ must divide $g(x)$.

Example 5.12. In this example, we are interested in 4-QM codes of length 20 over $\mathbb{F}_3$ with associated vector $a = (2, 1, 1, 2, 2) \in \mathbb{F}_3^5$. Let α be a primitive element of $\mathbb{F}_{3^4}$ with minimal polynomial $C_{f_\alpha}(x) = x^4 + 2x^3 + x^2 + 2x + 1 = 0$. Hence $B = \{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of the extension $\mathbb{F}_{3^4}/\mathbb{F}_3$. Let the irreducible factorization of $f_{\bar{a}}(x)$ be

$$\begin{aligned} f_{\bar{a}}(x) &= x^5 - 2 = (x+1) \cdot (x^4 + 2x^3 + x^2 + 2x + 1) \\ &= f_1(x)f_2(x). \end{aligned}$$

Then $\mathbb{E}_1 := \mathbb{F}_3[x]/\langle f_1(x) \rangle = \mathbb{F}_3$ and $\mathbb{E}_2 := \mathbb{F}_3[x]/\langle f_2(x) \rangle = \mathbb{F}_{3^4}$. Let C be the 4-QM code generated by $a(x) = (a_1(x), a_2(x), a_3(x), a_4(x)) \in R_{3,5}^4$, where

$$\begin{aligned} a_1(x) &= x^3 + x^2 \\ a_2(x) &= 2x^3 + 2x^2 \\ a_3(x) &= x^4 + 2x^3 + x + 2 \\ a_4(x) &= x^3 + 1 \end{aligned}$$

It follows that the constituent components of C are

$$\begin{aligned} C_1 &= \text{Span}_{\mathbb{E}_1}(a_1(-1), a_2(-1), a_3(-1), a_4(-1)) = \{0\} \subseteq \{0\}. \\ C_2 &= \text{Span}_{\mathbb{E}_2}\{(a_1(\alpha), a_2(\alpha), a_3(\alpha), a_4(\alpha))\} = \text{Span}_{\mathbb{E}_2}\{(1, 2, 2\alpha^3 + 2\alpha^2 + 2\alpha, 2\alpha^2 + \alpha)\} \subseteq \mathbb{E}_2^4. \end{aligned}$$

As $\gcd(4, 3) = 1$, the polynomials f_1 and f_2 are irreducible over $\mathbb{E}_1$ and $\mathbb{E}_2$ respectively. Recall that the companion matrix of $C_{f_\alpha}(x)$ is

$$C_{f_\alpha} = \begin{pmatrix} 0 & 0 & 0 & 2 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{pmatrix}$$

It follows that

$$C_{f_\alpha} C_2 = \text{Span}_{\mathbb{E}_2} \{ (2\alpha^3 + 2, 2\alpha^3 + \alpha^2 + 1, \alpha^3 + 2\alpha^2 + 2, \alpha^3 + 2\alpha^2 + 2\alpha + 2) \} \subseteq C_2$$

which means that $C = C_1 \oplus C_2 \subseteq \mathbb{E}_1^4 \oplus \mathbb{E}_2^4$ has an $\mathbb{F}_{3^4}$ -linear image with respect to the basis B .

6. Asymptotics

In this, we are interested in the performance of ℓ -QM codes. First recall that if $(F_n)_{n \in \mathbb{N}}$ is a family of codes of parameters $[n, k_n, d_n]$, the rate r and relative distance δ of $(F_n)_{n \in \mathbb{N}}$ are defined as

$$r = \lim_{n \rightarrow \infty} \sup \frac{k_n}{n} \quad \text{and} \quad \delta = \lim_{n \rightarrow \infty} \inf \frac{d_n}{n}.$$

A family $(F_n)_{n \in \mathbb{N}}$ is said to be **asymptotically good** if $r\delta > 0$.

Proposition 6.1. Let $C \subseteq$ be an ℓ -QM code of length $n = m\ell$, and let $d(C)$ be its Hamming distance. Then

$$d(C) \geq \frac{d(\Phi_B(C))}{\ell}.$$

Proof. Let $c(x) = (\tilde{c}_0(x), \tilde{c}_1(x), \dots, \tilde{c}_{\ell-1}(x))$ be a non zero element of $\varphi_{\bar{a}, \ell}(C)$, then

$$c'(x) = \Phi_B(c(x))e_i = \sum_{i=0}^{\ell-1} \tilde{c}_i(x)e_i = \sum_{i=0}^{\ell-1} \left(\sum_{j=0}^{m-1} \tilde{c}_{i,j}x^j \right) e_i = \sum_{j=0}^{m-1} \underbrace{\left(\sum_{i=0}^{\ell-1} \tilde{c}_{i,j}e_i \right)}_{c'_j} x^j \in \Phi_B(C).$$

Observe that $c'_j = \sum_{i=0}^{\ell-1} \tilde{c}_{i,j}e_i = 0$ implies that $\tilde{c}_{i,j} = 0$ for all $i = 0, \dots, \ell - 1$, since B is a basis. Thus

$$\sum_{i=0}^{\ell-1} w(\tilde{c}_{i,j}) \leq \ell w(c'_j), \quad j = 0, \dots, m - 1.$$

It follows that

$$w(c(x)) = \sum_{i=0}^{\ell-1} \sum_{j=0}^{m-1} w(\tilde{c}_{i,j}) \leq \ell \sum_{i=0}^{m-1} w(c'_j) = w(c'(x))$$

Finally,

$$d(C) \geq \frac{d(\Phi_B(C))}{\ell}.$$

□

In [1] the authors proved that t -CIS QPC codes (particular subclass of quasi-polycyclic codes) are asymptotically good. Similarly, in [14] M. Shi and others showed that ℓ -QT codes are asymptotically good. Following these two works, we prove that ℓ -QM codes and additive monomial codes are also asymptotically good. First recall that the q -ary entropy function is defined for $0 < y < \frac{q-1}{q}$ by,

$$H_q(y) = y \log_q(q-1) - y \log_q(y) - (1-y) \log_q(1-y).$$

We invite the reader to see [2, Chapter 2] for more details on the entropy function. Adapting the proof [1, Theorem 5.4] in the case t -CIS QP codes, we obtain the following result on ℓ -QM codes.

Proposition 6.2 (Similar to [1], Theorem 5.4). *For any fixed integer $\ell > 1$, there are infinite families of ℓ -QM codes length $n = m\ell$, rate $\frac{1}{\ell}$ and of relative distance δ , such that*

$$H_q(\delta) \geq \frac{\ell-1}{\ell}.$$

Proof. As each λ -constacyclic code of length m is a monomial code with associated vector $a = (1, \dots, 1, \lambda) \in \mathbb{F}_q^m$, the result it is obtained by [1, Theorem 5.4]. $\square$

Proposition 6.3 ([14]). *For any prime power q there are infinite families of additive monomial codes of length $m \rightarrow \infty$ over $\mathbb{F}_{q^\ell}$ of rate $\frac{1}{\ell}$ and relative distance*

$$\delta \geq \frac{1}{\ell} H_q^{-1}(1 - 1/\ell)$$

Proof. By [14, Theorem 3.4] and Proposition 6.1. $\square$

7. Conclusion

In this paper, we studied the structure of codes invariant under a monomial matrix $M = \text{diag}(a_0, a_1, \dots, a_{n-1})P_\sigma$ where σ is a permutation and P_σ is its associated permutation matrix, particularly the structure of monomial codes introduced in [4], where we view them as the ideals in the polynomial ring $R_{q,n}$, and we derive their polynomial characterization as in the case of cyclic codes. Secondly, we studied the algebraic and additive structure of ℓ -quasi-monomial codes, where we prove a one-to-one correspondence between them and $R_{n,q}$ -submodules of $R_{n,q}^\ell$. We characterize those codes that have $\mathbb{F}_{q^\ell}$ -linear images with respect to a basis of $\mathbb{F}_{q^\ell}/\mathbb{F}_q$, based on the CRT decomposition. Finally, we proved that quasi-monomial codes are asymptotically good. An important problem here is to study the structure of monomial codes as hyperinvariant subspaces, introduced in [6] for cyclic codes, and also to investigate their σ -LCD structure as in [3].

Acknowledgment: The authors would like to thank the reviewers for their comments and suggestions that allowed us to correct several errors and improve the readability and quality of the article.

References

- [1] A. Alahmadi, C. Guneri, H. Shoaib, P. Sole, Long quasi-polycyclic t -CIS codes, *Adv. Math. Commun.* 2(1) (2018) 189–198.
- [2] T. M. Cover, J. A. Thomas, *Elements of Information Theory*, Second Edition, (2006).
- [3] C. Carlet, S. Mesnager, C. Tang and Y. Qi, On σ -LCD codes, *IEEE Trans. Inf. Theory* 65(3) (2019) 1694–1704.

- [4] M. I. Garcia-Planas, M. D. Magret, L. Emilie, Monomial codes seen as invariant subspaces, *Open mathematics* 15(1) (2017) 1099–1107.
- [5] M.I. Garcia-Planas, M. D. Magret, Eigenvalues and eigenvectors of monomial matrices, *Proceedings of the XXIV Congress on Differential Equations and Applications/XIV Congress on Applied Mathematics*. Universidad de Cadiz (2015) 963–966 .
- [6] M. I. Garcia-Planas, M. D. Magret, M. E. Montoro, Cyclic codes as hyperinvariant subspaces, *Conference Proceedings 6th International Conference on Physics and Control*, (2013).
- [7] C. Guneri, F. Ozdemir, P. Sole, On the additive cyclic structure of quasi-cyclic codes, *Discrete Mathematics* 341 (2018) 2735–2741.
- [8] C. Guneri, F. Ozbudak, B. Ozkaya, E. Sacikara, Z. Sepasdar, P. Sole, Structure and performance of generalized quasi-cyclic codes, *Finite Fields Appl.* 47 (2017) 183–202 .
- [9] H. K. Hoffman, R. Kunze, *Linear Algebra*, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, (1971).
- [10] W.C. Huffman, V. Pless, *Fundamentals of Error Correcting Codes*, Cambridge University Press, (2003).
- [11] R.L. Lidl, H. Niederreiter, *Introduction to Finite Fields and their Applications* (rev. ed.), Cambridge University Press, Cambridge (1987).
- [12] H. Ou-azzou and M. Najmeddine, On the algebraic structure of polycyclic codes, *Filomat* 35(10) (2021) 3407–3421 .
- [13] D. Radkova, A.J. Van Zanten, Constacyclic codes as invariant subspaces, *Linear Algebra Appl.* 430 (2009) 855–864 .
- [14] M. Shi, R. Wu, P. Sole, Asymptotically good additive cyclic codes exist, *IEEE Communications Letters* 22(10) (2018) 1980–1983.
- [15] M. Shi, X. Li, Z. Sepasdar, P. Sole, Polycyclic codes as invariant subspaces, *Finite Fields Appl.* 68 (2020) 101760.