INTERNATIONAL ELECTRONIC JOURNAL OF ALGEBRA
VOLUME 33 (2023) 77-86
DOI: 10.24330/ieja.1198011

WHEN DO QUASI-CYCLIC CODES HAVE $\mathbb{F}_{q^l}$-LINEAR IMAGE?

Z. Pourshafiey and R. Nekooei

Received: 13 August 2021; Revised: 25 September 2022; Accepted: 25 September 2022
Communicated by Tuğçe Pekacar Çalcı

Dedicated to the memory of Professor Edmund R. Puczyłowski

ABSTRACT. A length ml, index l quasi-cyclic code can be viewed as a cyclic code of length m over the field $\mathbb{F}_{q^l}$ via a basis of the extension $\mathbb{F}_{q^l}/\mathbb{F}_q$. This cyclic code is an additive cyclic code. In [C. Güneri, F. Özdemir, P. Solé, On the additive cyclic structure of quasi-cyclic codes, Discrete. Math., 341 (2018), 2735-2741], authors characterize the (l,m) values for one-generator quasi-cyclic codes for which it is impossible to have an $\mathbb{F}_{q^l}$-linear image for any choice of the polynomial basis of $\mathbb{F}_{q^l}/\mathbb{F}_q$. But this characterization for some (l,m) values is very intricate. In this paper, by the use of this characterization, we give a more simple characterization.

Mathematics Subject Classification (2020): 94B15, 94B05
Keywords: Cyclic code, quasi-cyclic code, additive cyclic code, linear code

1. Introduction

Throughout this paper, q is a prime power, $\mathbb{F}_q$ denotes the finite field with q elements, m and l are positive integers such that $l > 1$ and $gcd(q,m) = 1$. A length ml, index l quasi-cyclic code is defined to be an $\mathbb{F}_q$-linear code in $\mathbb{F}_q^{ml}$ which is closed under T^l, where T is the shift operator defined by $T(c_0, c_1, \ldots, c_{ml-1}) = (c_{ml-1}, c_0, \ldots, c_{ml-2})$. A length ml, index l quasi-cyclic code C over $\mathbb{F}_q$ can be viewed as an $R(m,q)$-submodule of $R(m,q)^l$, where $R(m,q) = \mathbb{F}_q[x]/\langle x^m - 1\rangle$. Using a polynomial basis β of $\mathbb{F}_{q^l}/\mathbb{F}_q$ and the map ϕ_β defined in [2, Section 2], we map the quasi-cyclic code C to $R(m,q^l) = \mathbb{F}_{q^l}[x]/\langle x^m - 1\rangle$. We denote this image by $\phi_\beta(C)$ and it becomes an $R(m,q)$-submodule of $R(m,q^l)$. Equivalently, $\phi_\beta(C)$ is an $\mathbb{F}_q$-linear cyclic code of length m over $\mathbb{F}_{q^l}$. Such codes are called additive cyclic codes [1].

In [4,5], the following question was posed: when is the image under a basis extension of a quasi-cyclic code $\mathbb{F}_{q^l}$-linear, hence a classical cyclic code? In [2], the authors answered this question and characterized quasi-cyclic codes with an $\mathbb{F}_{q^l}$-linear image in $R(m,q^l)$. This characterization is particularly simple in the case of a one-generator quasi-cyclic code. They also characterized the (l,m) values for one-generator quasi-cyclic codes for which it is impossible to have an $\mathbb{F}_{q^l}$-linear image for any choice of the polynomial basis of $\mathbb{F}_{q^l}/\mathbb{F}_q$. But these conclusions should be checked for each case as in multiple steps (we will state this steps in Remark 2.1) and for some (l,m) values, these conclusions and characterizations are very intricate (in Example 2.2, we will show this intricacy for $q=2$, $m=3$ and $l=6$).

In this paper, by use of the characterizations and conclusions in [2], we give a more simple characterization to list the (l,m) values for one-generator quasi-cyclic codes for which it is impossible to have an $\mathbb{F}_{q^l}$-linear image for any choice of the polynomial basis of $\mathbb{F}_{q^l}/\mathbb{F}_q$. In Section 2, we assume that $l>1$ is a positive integer and m is a number with $gcd(q,m)=1$. We give a characterization of the list (l,m) values for one-generator quasi-cyclic codes for it is impossible to have an F_{q^l}-linear image for any choice of the polynomial basis $\mathbb{F}_{q^l}/\mathbb{F}_q$. In Section 3, we list some values (l,m) for one-generator quasi-cyclic codes for it is impossible to have an F_{q^l}-linear image for any choice of the polynomial basis $\mathbb{F}_{q^l}/\mathbb{F}_q$, such that for these values (l,m) we don't need to use the characterizations stated in Section 2 and it is sufficient to know the numbers l and m.

2. Relationship between $\mathbb{F}_{q^l}$-linear quasi-cyclic codes and $R(m,q)$

Throughout this section, l,m are positive integers such that $l>1$ and $gcd(q,m)=1$. Let $\sum(q)$ be the set of all (l,m) values for one-generator length ml, index l quasi-cyclic codes C for which it is impossible to have an $\mathbb{F}_{q^l}$-linear image $\phi_\beta(C)$, for any choice of the polynomial basis β. Let $x^m-1=f_1(x)\ldots f_s(x)$ be the decomposition of x^m-1 into irreducible polynomials of $\mathbb{F}_q[x]$. Suppose that $\deg f_i(x)=t_i$ $(1\le i\le s)$. Put $T_q(m)=\{t_1,\ldots,t_s\}$. Hence $R(m,q)\cong\mathbb{F}_{q^{t_1}}\oplus\cdots\oplus\mathbb{F}_{q^{t_s}}$.

In the following remark we use the notations in [2].

Remark 2.1. (i) Decompose $R(m,q)$ to field extensions $\mathbb{E}_i$ $(1\le i\le s)$ of $\mathbb{F}_q$.

(ii) Choice an irreducible polynomial $f_\alpha(x)\in\mathbb{F}_q[x]$ of degree l such that $f_\alpha(\alpha)=0$ and $\beta=\{1,\alpha,\ldots,\alpha^{l-1}\}$ be a basis of $\mathbb{F}_{q^l}/\mathbb{F}_q$.

(iii) For every i $(1\le i\le s)$ decompose $f_\alpha(x)\in\mathbb{F}_q[x]$ into irreducible polynomials $f_{\alpha,j}(x)\in\mathbb{E}_i$ $(1\le j\le b_i)$, where $[\mathbb{E}_i:\mathbb{F}_q]=t_i$ and $gcd(l,t_i)=b_i$.

(iv) Form companion matrix of $f_\alpha(x)$, i.e.

$$M_\alpha=\left[\ [\alpha.1]_\beta\quad[\alpha.\alpha]_\beta\quad[\alpha.\alpha^2]_\beta\quad\ldots\quad[\alpha.\alpha^{l-1}]_\beta\ \right].$$

(v) For every i $(1\le i\le s)$, compute the invariant subspaces W_i^j $(1\le j\le b_i)$, where $W_i^j=\{u\in\mathbb{E}_i^l\ \mid\ f_{\alpha,j}(M_\alpha)u=0\}$.

(vi) Find a non-trivial one-generator quasi-cyclic code $C=\langle c_0(x),c_1(x),\ldots,c_{l-1}(x)\rangle\subseteq R(m,q)^l$ such that each constituent $C_i=\langle(c_0(\xi^{u_i}),c_1(\xi^{u_i}),\ldots,c_{l-1}(\xi^{u_i}))\rangle$ $(1\le i\le s)$ of C, be a direct sum of $W_i^j s$, where by the above observations $\xi^m=1$ and $\mathbb{E}_i=\mathbb{F}_q[\xi^{u_i}]$.

If there exists such non-trivial one-generator quasi-cyclic code, it means $(l,m)\notin\sum(q)$. Otherwise, we should choose another basis β and check the above steps for basis β. If for every basis β of $\mathbb{F}_{q^l}/\mathbb{F}_q$ we can't find such quasi-cyclic code, it means $(l,m)\in\sum(q)$. For some values (l,m) to check these steps are very intricate. See the following example:

Example 2.2. If we want to see whether $(6,3) \in \sum(2)$ or not, we should check all steps in Remark 2.1 for every polynomial basis β of $\mathbb{F}_{2^6}/\mathbb{F}_2$. Hence we should find all irreducible polynomials of degree 6 in $\mathbb{F}_2[x]$ and it is very intricate. But as we will see, by Theorem 2.5, it is easy to see that $(6,3) \in \sum(2)$.

Lemma 2.3. *Let l, m be positive integers such that $l > 1$, $gcd(q,m) = 1$ and $T_q(m) = \{t_1, \ldots, t_s\}$. Suppose that for every i $(1 \le i \le s)$, $l \nmid t_i$. Then $(l,m) \in \sum(q)$.*

Proof. Suppose that there exist a length ml, index l one-generator quasi-cyclic code C and a polynomial basis β of $\mathbb{F}_{q^l}/\mathbb{F}_q$ such that $\phi_\beta(C)$ is $\mathbb{F}_{q^l}$-linear. We will show that $C = 0$. For a fixed i with $1 \le i \le s$, since $l \nmid t_i$, $gcd(l,t_i) = b_i \neq l$ and hence $\dfrac{l}{b_i} = d_i > 1$. By [2, Theorem 4.1(ii)] and the notation of this theorem $dim_{\mathbb{E}_i} C_i = k_i d_i$, for some $0 \le k_i \le b_i$. If $k_i \neq 0$, then $dim_{\mathbb{E}_i} C_i > 1$. But by the definition of C_i, $dim_{\mathbb{E}_i} C_i \le 1$, since C is a one-generator quasi-cyclic code. Hence $k_i = 0$ and so $C_i = 0$ $(1 \le i \le s)$. Therefore $C = 0$ and hence $(l,m) \in \sum(q)$. □

Proposition 2.4. *Let l, m be positive integers such that $l > 1$, $gcd(q,m) = 1$ and $T_q(m) = \{t_1, \ldots, t_s\}$. Suppose that there exists i $(1 \le i \le s)$ such that $l|t_i$. Then $(l,m) \notin \sum(q)$.*

Proof. We will prove that there exists a non-trivial one-generator quasi-cyclic code of length ml, with index l. $C = \langle c_0(x), c_1(x), \ldots, c_{l-1}(x)\rangle \subseteq R(m,q)^l$ such that $\phi_\beta(C)$ is $\mathbb{F}_{q^l}$-linear, for some polynomial basis β of $\mathbb{F}_{q^l}/\mathbb{F}_q$. Let $\beta = \{1, \alpha, \ldots, \alpha^{l-1}\}$ be a basis of $\mathbb{F}_{q^l}/\mathbb{F}_q$ and $\mathbb{F}_{q^l} = \mathbb{F}_q[x]/\langle f_\alpha(x)\rangle$ such that $f_\alpha(x) \in \mathbb{F}_q[x]$ is irreducible, $\deg f_\alpha(x) = l$ and $f_\alpha(\alpha) = 0$. Let $f_\alpha(x) = x^l + a_{l-1}x^{l-1} + \cdots + a_1 x + a_0 \in \mathbb{F}_q[x]$. Hence the companion matrix of $f_\alpha(x)$ is

$$M_\alpha = \begin{bmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{l-1} \end{bmatrix}.$$

By the notations of [2, Section 2], we have $\mathbb{E}_i = \mathbb{F}_q[\xi_i]$, where $\xi_i = \xi^{u_i}$ and $\xi^m = 1$. Since $[\mathbb{E}_i : \mathbb{F}_q] = t_i$ and $l|t_i$, there exists $d \in \mathbb{N}$ such that $t_i = ld$. Hence there exists an irreducible polynomial $\lambda(x) \in \mathbb{F}_{q^l}[x]$ of degree d such that $\mathbb{E}_i \cong \mathbb{F}_{q^l}[x]/\langle\lambda(x)\rangle$. So there exists a root δ of $\lambda(x)$ such that $\mathbb{E}_i \cong \mathbb{F}_{q^l}[\delta]$ and hence $\mathbb{F}_{q^l}$ is embedded in $\mathbb{E}_i$. Now since $\alpha \in \mathbb{F}_{q^l}$, there exists $\omega \in \mathbb{E}_i$ such that $f_\alpha(\omega) = 0$ and hence $x - \omega | f_\alpha(x)$ in $\mathbb{E}_i[x]$. In this case, by the observations in [2, Section 4], we have $b_i = l$ and $d_i = 1$. Now we constitute $\mathbb{E}_i$-subspace W_i^1 for $f_{\alpha,1}(x) = x - \omega$. Hence we have $W_i^1 = \{u \in \mathbb{E}_i^l \mid (M_\alpha - \omega I)u = 0\}$. By the observations above [2, Theorem 4.1], $dim_{\mathbb{E}_i} W_i^1 = \deg f_{\alpha,1}(x) = \deg(x - \omega) = 1$, and so there exist $g_k(x) \in F_q[x]$ $(0 \le k \le l-1)$ such that $W_i^1 = \langle g_0(\omega), \ldots, g_{l-1}(\omega)\rangle$. Since $\omega \in \mathbb{E}_i$, $g_k(\omega) \in \mathbb{E}_i = \mathbb{F}_q[\xi_i]$ $(0 \le k \le l-1)$ and hence, for every k $(0 \le k \le l-1)$, there exist

$h_k(x) \in \mathbb{F}_q[x]$ such that $g_k(\omega) = h_k(\xi_i)$ $(0 \le k \le l-1)$. Now let $\theta(x) = \prod_{i \neq j=1}^{s} f_j(x)$. We have $gcd(f_i(x), \theta(x)) = 1$. Since $\mathbb{F}_q[x]$ is a PID, there exist $\psi(x), \psi'(x) \in \mathbb{F}_q[x]$ such that $\psi(x)f_i(x) + \psi'(x)\theta(x) = 1$. Set $c_k(x) = \theta(x)\psi'(x)h_k(x)$. Now we have $C_j = \langle c_0(\xi_j), \ldots, c_i(\xi_j), \ldots, c_{l-1}(\xi_j)\rangle$ $(1 \le j \le s)$. Let $j \neq i$ and $1 \le j \le s$. Since $f_j(\xi_j) = 0$, $\theta(\xi_j) = 0$ and hence $c_k(\xi_j) = \theta(\xi_j)\psi'(\xi_j)h_k(\xi_j) = 0$ $(0 \le k \le l-1)$. Therefore for every $j \neq i$ and $1 \le j \le s$, $C_j = 0$. Let $j = i$. Since $f_i(\xi_i) = 0$, $c_k(\xi_i) = \theta(\xi_i)\psi'(\xi_i)h_k(\xi_i) = (1 - f_i(\xi_i)\psi(\xi_i))h_k(\xi_i) = h_k(\xi_i) = g_k(\omega)$ $(0 \le k \le l-1)$. Therefore $C_i = W_i^1$, and so $C = C_1 \oplus \cdots \oplus C_{i-1} \oplus C_i \oplus C_{i+1} \oplus \cdots \oplus C_{l-1} = 0 \oplus \cdots \oplus 0 \oplus W_i^1 \oplus 0 \oplus \cdots \oplus 0 = W_i^1$. Then, by the observation above [2, Theorem 4.1], C is $\mathbb{F}_{q^l}$-linear, and so $(l,m) \notin \sum(q)$. □

Theorem 2.5. *Let l, m be positive integers such that $l > 1$, $gcd(q,m) = 1$ and $T_q(m) = \{t_1, \ldots, t_s\}$. Then $(l,m) \in \sum(q)$ if and only if, for every i $(1 \le i \le s)$, $l \nmid t_i$.*

Proof. It follows from Lemma 2.3 and Proposition 2.4. □

Set $D_q(m) = \{l \;:\; 1 \neq l \in \mathbb{N},\; l \mid t_i, \text{ for some } i \ (1 \le i \le s)\}$.

Corollary 2.6. *Let l, m be positive integers such that $l > 1$ and $gcd(q,m) = 1$. We have:*

(i) $(l,m) \in \sum(q)$ *if and only if* $l \notin D_q(m)$.

(ii) *For every* $l \ge m$, $(l,m) \in \sum(q)$.

Proof. (i) It is clear from Theorem 2.5.

(ii) Clearly for every $l \ge m$, $l \notin D_q(m)$, and so by part(i), $(l,m) \in \sum(q)$. □

Example 2.7.

(i) Let $q = 2$ and $m = 9$. We have $x^9 - 1 = (x-1)(x^2+x+1)(x^6+x^3+1)$, and so $T_2(9) = \{1,2,6\}$ and $D_2(9) = \{2,3,6\}$. Hence by Corollary 2.6, $(2,9), (3,9), (6,9) \notin \sum(2)$ and, for every $l \notin \{2,3,6\}$, $(l,9) \in \sum(2)$.

(ii) Let $q = 2$ and $m = 37$. We have $x^{37} - 1 = (x-1)(x^{36}+x^{35}+x^{34}+\cdots+x^2+x+1)$, and so $T_2(37) = \{1,36\}$ and $D_2(37) = \{2,3,4,6,9,12,18,36\}$. Hence by Corollary 2.6, $(2,37), (3,37), (4,37), (6,37), (9,37), (12,37), (18,37), (36,37) \notin \sum(2)$ and for every $l \notin \{2,3,4,6,9,12,18,36\}$, $(l,37) \in \sum(2)$.

In the following tables, for the convenience of the reader, we list the set $T_2(m)$ for odd m values up to 73 and $T_3(m)$ for m values up to 43 with $gcd(m,3) = 1$.

m	$T_2(m)$	m	$T_2(m)$	m	$T_2(m)$	m	$T_2(m)$
3	$\{1,2\}$	21	$\{1,2,3,6\}$	39	$\{1,2,12\}$	57	$\{1,2,18\}$
5	$\{1,4\}$	23	$\{1,11\}$	41	$\{1,20\}$	59	$\{1,58\}$
7	$\{1,3\}$	25	$\{1,4,20\}$	43	$\{1,14\}$	61	$\{1,60\}$
9	$\{1,2,6\}$	27	$\{1,2,6,18\}$	45	$\{1,2,4,6,12\}$	63	$\{1,2,3,6\}$
11	$\{1,10\}$	29	$\{1,28\}$	47	$\{1,23\}$	65	$\{1,4,12\}$
13	$\{1,12\}$	31	$\{1,5\}$	49	$\{1,3,21\}$	67	$\{1,66\}$
15	$\{1,2,4\}$	33	$\{1,2,10\}$	51	$\{1,2,8\}$	69	$\{1,2,11,22\}$
17	$\{1,8\}$	35	$\{1,3,4,12\}$	53	$\{1,52\}$	71	$\{1,35\}$
19	$\{1,18\}$	37	$\{1,36\}$	55	$\{1,4,10,20\}$	73	$\{1,9\}$

m	$T_3(m)$	m	$T_3(m)$	m	$T_3(m)$	m	$T_3(m)$
2	$\{1\}$	13	$\{1,3\}$	23	$\{1,11\}$	34	$\{1,16\}$
4	$\{1,2\}$	14	$\{1,6\}$	25	$\{1,4,20\}$	35	$\{1,4,6,12\}$
5	$\{1,4\}$	16	$\{1,2,4\}$	26	$\{1,3\}$	37	$\{1,18\}$
7	$\{1,6\}$	17	$\{1,16\}$	28	$\{1,2,6\}$	38	$\{1,18\}$
8	$\{1,2\}$	19	$\{1,18\}$	29	$\{1,28\}$	40	$\{1,2,4\}$
10	$\{1,4\}$	20	$\{1,2,4\}$	31	$\{1,30\}$	41	$\{1,8\}$
11	$\{1,5\}$	22	$\{1,5\}$	32	$\{1,2,4,8\}$	43	$\{1,42\}$

Example 2.8. Let $\Omega = \bigcup\{D_2(m) \mid m \leq 73, m \text{ is odd }\} = \{2,3,4,5,6,7,8,9,10,11, 12,13,14,15,18,20,21,22,23,26,28,29,30,33,35,36,52,58,60,66\}$. By Corollary 2.6, for every number $1 \neq l \notin \Omega$ and every odd number $m \leq 73$, we have $(l,m) \in \sum(2)$. In the following table, for every $l \in \Omega$, we list the odd m values up to 73 such that $(l,m) \in \sum(2)$.

l	m
2	7,23,31,47,49,71,73
3	3,5,11,15,17,23,25,29,31,33,41,43,47,51,53,55,59,69,71
4	3,7,9,11,19,21,23,27,31,33,43,47,49,57,59,63,67,69,71,73
5	3,5,7,9,13,15,17,19,21,23,27,29,35,37,39,43,45,47,49,51,53,57, 59,63,65,67,69,71,73
6	3,5,7,11,15,17,23,25,29,31,33,41,43,47,49,51,53,55,59,69,71,73
7	3,5,7,9,11,13,15,17,19,21,23,25,27,31,33,35,37,39,41,45,47,51,53,55,57, 59,61,63,65,67,69,73
8	3,5,7,9,11,13,15,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49,51,53, 55,57,59,61,63,65,67,69,71,73
9	3,5,7,9,11,13,15,17,21,23,25,29,31,33,35,39,41,43,45,47,49,51,53,55, 59,61,63,65,67,69,71
10	3,5,7,9,13,15,17,19,21,23,27,29,31,35,37,39,43,45,47,49,51,53,57,59, 63,65,67,69,71,73
11	3,5,7,9,11,13,15,17,19,21,25,27,29,31,33,35,37,39,41,43,45,47,49,51, 53,55,57,59,61,63,65,71,73
12	3,5,7,9,11,15,17,19,21,23,25,27,29,31,33,41,43,47,49,51,53,55,57,59, 63,67,69,71,73
13	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,55,57,59,61,63,65,67,69,71,73
14	3,5,7,9,11,13,15,17,19,21,23,25,27,31,33,35,37,39,41,45,47,49,51,53, 55,57,59,61,63,65,67,69,71,73

l	m
15	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,63,65,67,69,71,73
18	3,5,7,9,11,13,15,17,21,23,25,29,31,33,35,39,41,43,45,47,49, 51,53,55,59,61,63,65,67,69,71,73
20	3,5,7,9,11,13,15,17,19,21,23,27,29,31,33,35,37,39,43,45,47,49, 51,53,57,59,63,65,67,69,71,73
21	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47, 51,53,55,57,59,61,63,65,67,69,71,73
22	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,61,63,65,71,73
23	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,49, 51,53,55,57,59,61,63,65,67,69,71,73
26	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,55,57,59,61,63,65,67,69,71,73
28	3,5,7,9,11,13,15,17,19,21,23,25,27,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,61,63,65,67,69,71,73
29	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,61,63,65,67,69,71,73
30	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,63,65,67,69,71,73
33	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,61,63,65,69,71,73

l	m
35	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,61,63,65,67,69,73
36	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,39,41,43,45,47,49, 51,53,55,57,59,61,63,65,67,69,71,73
52	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,55,57,59,61,63,65,67,69,71,73
58	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,61,63,65,67,69,71,73
60	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,63,65,67,69,71,73
66	3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33,35,37,39,41,43,45,47,49, 51,53,55,57,59,61,63,65,69,71,73

Example 2.9. Let $\Omega = \bigcup\{D_3(m) | m \leq 43, gcd(m,3) = 1\} = \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 20, 21, 28, 30, 42\}$. By Corollary 2.6, for every number $1 \neq l \notin \Omega$ and every $m \leq 43$ with $gcd(m,3) = 1$, we have $(l,m) \in \sum(3)$. In the following table, for every $l \in \Omega$, we list m values up to 43 with $gcd(m,3) = 1$ such that $(l,m) \in \sum(3)$.

l	m
2	2,11,13,22,23,26
3	2,4,5,8,10,11,16,17,20,22,23,25,29,32,34,40,41
4	2,4,7,8,11,13,14,19,22,23,26,28,31,37,38,42
5	2,4,5,7,8,10,13,14,16,17,19,20,23,26,28,29,32,34,35,37,38,40,41,43
6	2,4,5,8,10,11,13,16,17,20,22,23,25,26,29,32,34,40,41
7	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,31,32,34,35,37,38,40,41
8	2,4,5,7,8,10,11,13,14,16,19,20,22,23,25,26,28,29,31,35,37,38,40,43
9	2,4,5,7,8,10,11,13,14,16,17,20,22,23,25,26,28,29,31,32,34,35,40,41,43
10	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,26,28,29,32,34,35,37,38,40,41,43
11	2,4,5,7,8,10,11,13,14,16,17,19,20,22,25,26,28,29,31,32,34,35,37,38,40,41,43
12	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,29,31,32,34,37,38,40,41,43
14	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,31,32,34,35,37,38,40,41
15	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,29,32,34,35,37,38,40,41,43
16	2,4,5,7,8,10,11,13,14,16,19,20,22,23,25,26,28,29,31,32,35,37,38,40,41,43
18	2,4,5,7,8,10,11,13,14,16,17,20,22,23,25,26,28,29,31,32,34,35,40,41,43
20	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,26,28,29,31,32,34,35,37,38,40,41,43
21	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,29,31,32,34,35,37,38,40,41
28	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,31,32,34,35,37,38,40,41,43
30	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,29,32,34,35,37,38,40,41,43
42	2,4,5,7,8,10,11,13,14,16,17,19,20,22,23,25,26,28,29,31,32,34,35,37,38,40,41

3. Relationship between $\mathbb{F}_{q^l}$-linear quasi-cyclic codes and values (l, m)

In this section, without using the decomposition of $R(m, q)$, we prepare a list of some values of (l, m) that shows whether (l, m) is in $\sum(q)$ or not.

Definition 3.1. Let m be co-prime to q. The cyclotomic coset of q (or q-cyclotomic coset) modulo m containing i is defined by $D_i = \{i.q^j (\text{mod } m) \in \mathbb{Z}_m \mid j = 0, 1, \dots\}$. A subset $\{i_1, \dots, i_k\}$ of $\mathbb{Z}_m$ is called a complete set of representatives of cyclotomic cosets of q modulo m if $D_{i_1}, \dots, D_{i_k}$ are distinct and $\bigcup_{j=1}^{k} D_{i_j} = \mathbb{Z}_m$.

Lemma 3.2. *Let $\{s_1, \dots, s_k\}$ be a complete set of representatives of cyclotomic cosets of q modulo $q^n - 1$. Then, for i with $1 \leq i \leq k$, $|D_{s_i}| \mid n$.*

Proof. Set $|D_{s_i}| = t_i$ $(1 \leq i \leq k)$. For a fixed i with $1 \leq i \leq k$, we prove $t_i | n$. By Definition 3.1, t_i is the minimal number such that $s_i q^{t_i} \equiv s_i (\text{mod } q^n - 1)$. By using the division algorithm, there exist unique numbers $a_i, b_i \in \mathbb{N}$ with $0 \leq b_i \leq t_i - 1$ such that $n = a_i t_i + b_i$. Since $s_i q^{t_i} \equiv s_i (\text{mod } q^n - 1)$, it is easy to see that $s_i \equiv s_i q^n \equiv s_i q^{b_i} (\text{mod } q^n - 1)$. Since t_i is minimal , $b_i = 0$ and so $t_i | n$ $(1 \leq i \leq k)$. $\square$

Proposition 3.3. *Let $m | q^n - 1$, for some $n \geq 1$ and n be minimal. Then $D_q(m) = \{l \ : \ 1 \neq l \in \mathbb{N}, \ l \mid n\}$.*

Proof. Let $\{s_1, \dots, s_k\}$ be a complete set of representatives of cyclotomic cosets of q modulo m and $d = \frac{q^n-1}{m}$. Suppose that $D_{ds_i}(1 \le i \le k)$ are some cyclotomic cosets of q modulo q^n-1. Put $|D_{ds_i}| = t_i$ $(1 \le i \le k)$. By [3, Theorem 3.4.11 and Remark 3.4.9(i)], we have $T_q(m) = \{t_1, \dots, t_k\}$. By Lemma 3.2, $t_i|n$ $(1 \le i \le k)$ and so $D_q(m) \subseteq \{l \,:\, 1 \neq l \in \mathbb{N},\ l \mid n\}$. Conversely, let $1 \neq l|n$. We will prove that $l \in D_q(m)$. Without loss of generality, we may assume that $s_1 = 0$ and $s_2 = 1$. Then $|D_{ds_2}| = |D_d| = t_2$. Since $t_2|n$, $t_2 \le n$. We will prove $t_2 = n$. By Definition 3.1, t_2 is the minimal number such that $dq^{t_2} \equiv d(\text{mod } q^n-1)$. Since $q^n-1 = md$, $m|q^{t_2}-1$ and, since n is minimal, $t_2 = n$. Then $n \in T_q(m)$. Now, by the definition of $D_q(m)$, $l \in D_q(m)$ and the proof is complete. □

Corollary 3.4. *Let l, m be positive integers such that $l > 1$. Suppose that $n \ge 1$ is a positive integer such that is minimal with respect to $m|q^n-1$. Then $(l,m) \in \sum(q)$ if and only if $l \nmid n$.*

Proof. It follows by Corollary 2.6 and Proposition 3.3. □

Example 3.5.
(i) Let $m = 1023$. Since $1023 = 2^{10}-1$, by Corollary 3.4, $(l, 1023) \in \sum(2)$ if and only if $l \notin \{2, 5, 10\}$.
(ii) Let $m = 51$. We have $51|2^8-1$ and 8 is minimal. By Corollary 3.4, $(l, 51) \in \sum(2)$ if and only if $l \notin \{2, 4, 8\}$.

Let $A(q) = \{m \in \mathbb{N} \mid m \mid q^{m-1}-1 \text{ and } m \nmid q^n-1, \text{ for all } n < m-1\}$.

Corollary 3.6. *Let $k \in A(q)$ and $m \equiv k(\text{mod } qk)$. Then for every l, such that $l|k-1$, $(l,m) \notin \sum(q)$.*

Proof. Let $k \in A(q)$ and $m \equiv k(\text{mod } qk)$. So there exists $t \in \mathbb{N}$ such that $m = qtk+k$. Hence $x^m-1 = (x-1)(x^{qtk+k-1} + x^{qtk+k-2} + \cdots + x^2 + x + 1)$. Let $f(x) = x^{k-1} + \cdots + x^2 + x + 1$. Since $k \in A(q)$, the cyclotomic cosets of q modulo k are $C_0 = \{0\}$ and $C_1 = \{1, q, \dots, q^{k-2}\}$. So $\{0, 1\}$ is a complete set of representatives of cyclotomic cosets of q modulo k. Therefore, by [3, Corollary 3.4.12], the number of monic irreducible factors of x^k-1 over $\mathbb{F}_q$ is equal to 2. Then $x^k-1 = (x-1)f(x)$, and so $f(x) \in \mathbb{F}_q[x]$ is irreducible. Let $g(x) = x^{qtk+k-1} + x^{qtk+k-2} + \cdots + x^2 + x + 1$ and $h(x) = x^{qtk} + x^{(qt-1)k} + \cdots + x^{2k} + x^k + 1$. We have $g(x) = f(x)h(x)$, and so $f(x)|g(x)$. Hence $f(x)|x^m-1$. Now, since $\deg f(x) = k-1$, $k-1 \in T_q(m)$ and the proof follows by Proposition 2.4. □

Example 3.7.
(i) In Example 2.7(ii), since $37 \in A(2)$, by Corollary 3.6, without the decomposition of $x^{37}-1$, we have
$(2,37), (3,37), (4,37), (6,37), (9,37), (12,37), (18,37), (36,37) \notin \sum(2)$ and for every $l \notin \{2,3,4,6,9,12,18,36\}, (l,37) \in \sum(2)$.
(ii) It is easy to see that $3 \in A(2)$. Let $M = \{m \mid gcd(m,2) = 1 \text{ and } m \equiv 3(\text{mod } 6)\}$. We have $M = \{3, 9, 15, 21, 27, \dots\}$. Since $2|2 = 3-1$, by Corollary 3.6, for every $m \in M$, $(2,m) \notin \sum(2)$.

4. Conclusion

Let l, m, q be positive integers such that q be a prime power, $l > 1$ and $gcd(m, q) = 1$. In this paper, we characterize all (l, m) values for quasi-cyclic codes C with one-generator, length ml and index l, for which it is impossible to have an F_{q^l}-linear image $\phi_\beta(C)$ for any choice of the polynomial basis β. We denote these all (l, m) values by $\sum(q)$. Suppose that the positive integers l, m, q be given. We want to see $(l, m) \in \sum(q)$ or not? At first we decompose the polynomial $x^m - 1 \in F_q[x]$ into irreducible polynomials $f_1(x), f_2(x), \ldots, f_s(x)$ of $F_q[x]$ with $\deg f_i(x) = t_i, (1 \leq i \leq s)$. Then we prove that $(l, m) \in \sum(q)$ if and only if, for every $i(1 \leq i \leq s)$, $l \nmid t_i$.

Acknowledgment. The authors would like to thank the referee for the valuable suggestions and comments.

References

[1] J. Bierbrauer, *The theory of cyclic codes and a generalization to additive codes*, Des. Codes Cryptogr., 25(2) (2002), 189-206.

[2] C. Güneri, F. Özdemir and P. Solé, *On the additive cyclic structure of quasi-cyclic codes*, Discrete. Math., 341(10) (2018), 2735-2741.

[3] S. Ling and C. Xing, Coding Theory, Cambridge University Press, 2004.

[4] M. Shi, J. Tang, M. Ge, L. Sok and P. Solé, *A special class of quasi-cyclic codes*, Bull. Aust. Math. Soc., 96(3) (2017), 513-518.

[5] M. Shi, R. Wu and P. Solé, *Long cyclic codes are good*, arXiv: 1709.09865v3 [cs.IT], 17 oct 2017, 1-5.

R. Nekooei (Corresponding Author) and **Z. Pourshafiey**
Faculty of Mathematics and Computer
Mahani Mathematical Research Center
Shahid Bahonar University of Kerman
Kerman, Iran
e-mails: rnekooei@uk.ac.ir (R. Nekooei)
zhpoorshafiee@gmail.com (Z. Pourshafiey)