A Relation Between Quasi-Cyclic Codes and 2-D Cyclic Codes

Cem Guneri, Ferruh Ozbudak

A Relation Between Quasi-Cyclic Codes and 2-D Cyclic Codes*

Cem Güneri[1] and Ferruh Özbudak[2]

[1] Sabancı University, FENS, 34956, Istanbul, Turkey
guneri@sabanciuniv.edu
[2] Middle East Technical University, Department of Mathematics and Institute of Applied Mathematics , 06531, Ankara, Turkey
ozbudak@metu.edu.tr

Abstract. We consider a q-ary quasi-cyclic code C of length $m\ell$ and index ℓ, where both m and ℓ are relatively prime to q. If the constituents of C are cyclic codes, we show that C can also be viewed as a 2-D cyclic code of size $m \times \ell$ over $\mathbb{F}_q$. If we further assume that m and ℓ are also coprime to each other, then we easily observe that the code C must be equivalent to a cyclic code. The last fact was proved earlier by Lim using a different approach.

1 Introduction and Background

Both 2-D cyclic codes and quasi-cyclic (q.-c.) codes are generalizations of cyclic codes. We introduce definitions and basic facts about these codes in this section. Although there are numerous useful references on both classes of codes, we refer to [2, 5] since our presentation will follow the notation and approach in these articles.

Let $\mathbb{F}_q$ be the finite field with q elements. **We assume throughout that $m, \ell > 1$ are integers both of which are relatively prime to q.** Let C be a linear code over $\mathbb{F}_q$ of length $m\ell$ whose codewords are viewed as $m \times \ell$ arrays, i.e. $c \in C$ is written as

$$c = \begin{pmatrix} c_{00}, \ldots, c_{0,\ell-1} \\ c_{10}, \ldots, c_{1,\ell-1} \\ \vdots \\ c_{m-1,0}, \ldots, c_{m-1,\ell-1} \end{pmatrix}. \tag{1}$$

If C is closed under row and column shift of codewords, then we call C a *2-D cyclic code of size* $m \times \ell$. As in the case of cyclic codes, we have a polynomial

* The authors were partially supported by TÜBİTAK under Grant No. TBAG-109T672.

(ideal) representation for 2-D cyclic codes. For this, consider the following $\mathbb{F}_q$-space isomorphism

$$\begin{aligned} \mathbb{F}_q^{m\times\ell} &\longrightarrow \mathbb{F}_q[x,y]/(x^m-1, y^\ell-1) \\ (a_{ij}) &\longmapsto \sum_{i=0}^{m-1}\sum_{j=0}^{\ell-1} a_{ij}x^i y^j, \end{aligned} \tag{2}$$

where $\mathbb{F}_q^{m\times\ell}$ denotes the space of all $m\times\ell$ arrays. Via this identification we can conclude that a linear subspace C of $\mathbb{F}_q^{m\times\ell}$ is 2-D cyclic if and only if C is an ideal when viewed as a subset of $\mathbb{F}_q[x,y]/(x^m-1, y^\ell-1)$. Note that we can also think of a 2-D cyclic code as an ideal of the group algebra $\mathbb{F}_q[\mathbb{Z}_m \times \mathbb{Z}_\ell]$.

Let η be a primitive ℓ^{th} root of unity and ξ be a primitive m^{th} of root unity in the rest of this document. We take both of these elements in some extension $\mathbb{F}$ of $\mathbb{F}_q$. Consider the following set:

$$\Omega = \{(\xi^i, \eta^j);\ 0 \le i \le m-1,\ 0 \le j \le \ell-1\}. \tag{3}$$

We define the $\mathbb{F}_q$-*conjugacy class containing* (ξ^i, η^j) to be

$$[(\xi^i,\eta^j)] = \left\{(\xi^i,\eta^j),(\xi^{iq},\eta^{jq}),\ldots,(\xi^{iq^{\delta-1}},\eta^{jq^{\delta-1}})\right\}, \tag{4}$$

where δ is the least common multiple of the degrees of ξ^i and η^j over $\mathbb{F}_q$.

Since a 2-D cyclic code C is an ideal of $\mathbb{F}_q[x,y]/(x^m-1, y^\ell-1)$, we can write it as $J/(x^m-1, y^\ell-1)$ for some ideal J of $\mathbb{F}_q[x,y]$. We define the *zero set* $Z(C)$ *of* C as the set of zeros of the ideal J over the algebraic closure $\bar{\mathbb{F}}_q$. Note that an $\mathbb{F}_q$-conjugacy class of an element $(\xi^i, \eta^j) \in \Omega$ can be described by any member of the class $[(\xi^i, \eta^j)]$. The set formed by picking exactly one representative from each conjugacy class in $Z(C)$ is called *a basic zero set for* C and denoted by $BZ(C)$. Since J contains the ideal $(x^m-1, y^\ell-1)$, its zeros lie in the set Ω. It can be shown that $Z(C)$ is a disjoint union of some $\mathbb{F}_q$-conjugacy classes of elements in Ω. Moreover, $Z(C)$ (hence $BZ(C)$) uniquely determines the code C and $\dim(C) = |\Omega \setminus Z(C)|$. It is easy to observe that the dual $C^\perp$ (with respect to the usual Euclidean inner product) of a 2-D cyclic code is also 2-D cyclic. The zero set of $C^\perp$ is related to that of C by the formula $Z(C^\perp) = \Omega \setminus Z(C)^{-1}$, where

$$Z(C)^{-1} := \left\{(\xi^{-i}, \eta^{-j}) : (\xi^i, \eta^j) \in Z(C)\right\}.$$

A linear code $C \subset \mathbb{F}_q^{m\ell}$ is called *quasi-cyclic of index* ℓ if it is invariant under shift of codewords by ℓ units. Note that a q.-c. code of index 1 is nothing but a usual cyclic code. We note that our notation will be the same as the notation of [5].

Remark 1. It is advantageous to think of length $m\ell$ codewords of a q.-c. as $m\times\ell$ arrays as in (1) since one immediately realizes that being closed under shift by ℓ units amounts to being closed under row shift. Hence, we also see clearly that any 2-D cyclic code of size $m\times\ell$ is a q.-c. code of length $m\ell$ and index ℓ.

Define the ring $R := \mathbb{F}_q[Y]/(Y^m - 1)$ and recall that a linear code of length ℓ over R is nothing but an R-submodule of R^ℓ. Consider the map

$$\begin{array}{lcl} \phi: & \mathbb{F}_q^{m\ell} & \longrightarrow R^\ell \\ c = & \begin{pmatrix} c_{00}, \ldots, c_{0,\ell-1} \\ c_{10}, \ldots, c_{1,\ell-1} \\ \vdots \\ c_{m-1,0}, \ldots, c_{m-1,\ell-1} \end{pmatrix} & \longmapsto (c_0(Y), c_1(Y), \ldots, c_{\ell-1}(Y)), \end{array} \tag{5}$$

where

$$c_j(Y) := \sum_{i=0}^{m-1} c_{ij} Y^i = c_{0j} + c_{1j} Y + c_{2j} Y^2 + \cdots + c_{m-1,j} Y^{m-1} \in R$$

for each $0 \leq j \leq \ell - 1$. In other words, we construct an element of R from each column of c. The map ϕ induces a one-to-one correspondence between index ℓ q.-c. codes of length $m\ell$ over $\mathbb{F}_q$ and linear codes of length ℓ over R. For the case $\ell = 1$, this amounts to the well-known polynomial (ideal) presentation of cyclic codes in R.

Next, we try to understand the structure of the ring R better. Since m is relatively prime to q, polynomial $Y^m - 1$ is separable. Let

$$Y^m - 1 = f_1 f_2 \ldots f_r \tag{6}$$

be its unique factorization into irreducible polynomials in $\mathbb{F}_q[Y]$. Taking reciprocal polynomials of both sides above we obtain

$$Y^m - 1 = -f_1^* f_2^* \ldots f_r^*, \tag{7}$$

where f_i^* denotes the reciprocal of f_i. Using the fact that the reciprocal of an irreducible polynomial is also irreducible, we see that equations (6) and (7) are two factorizations of the same polynomial into irreducibles. We rewrite $Y^m - 1$ as

$$Y^m - 1 = \delta g_1 g_2 \ldots g_s h_1 h_1^* \ldots h_t h_t^*, \tag{8}$$

where g_i's are those f_j's which are associate to their own reciprocals and h_i, h_i^*'s are the remaining f_j's grouped in pairs (so, $2t + s = r$). Note that for a primitive m^{th} root of unity ξ, the roots of irreducible factors in (8) are powers of ξ.

By Chinese Remainder Theorem we have

$$R = \left(\bigoplus_{i=1}^{s} \mathbb{F}_q[Y]/(g_i) \right) \oplus \left(\bigoplus_{j=1}^{t} \mathbb{F}_q[Y]/(h_j) \oplus \mathbb{F}_q[Y]/(h_j^*) \right). \tag{9}$$

We will use the following notation for the direct factors above:

$$G_i = \mathbb{F}_q[Y]/(g_i) \quad H_j^{'} = \mathbb{F}_q[Y]/(h_j) \quad H_j^{''} = \mathbb{F}_q[Y]/(h_j^*)$$

Since the polynomials are irreducible, each of the quotients above are finite fields (e.g. $[G_i : \mathbb{F}_q] = \deg g_i$).

Note that (9) implies

$$R^\ell = \left(\bigoplus_{i=1}^{s} G_i^\ell \right) \oplus \left(\bigoplus_{j=1}^{t} (H_j^{'})^\ell \oplus (H_j^{''})^\ell \right). \tag{10}$$

Hence, any linear code C of length ℓ over R can be decomposed as

$$C = \left(\bigoplus_{i=1}^{s} C_i \right) \oplus \left(\bigoplus_{j=1}^{t} C_j^{'} \oplus C_j^{''} \right), \tag{11}$$

where $C_i, C_j^{'}, C_j^{''}$ are linear codes of length ℓ over the fields $G_i, H_j^{'}, H_j^{''}$, respectively. These length ℓ linear codes over various extensions of $\mathbb{F}_q$ are called the *constituents of* C.

In [2, Theorem 4.3], a trace representation for 2-D cyclic codes is obtained starting with a basic zero set of the dual code. In [5, Theorem 5.1], a trace representation for q.-c. codes is obtained based on the decomposition in (9) and the constituent codes. Both results are extensions of the following well-known trace representation of cyclic codes.

Theorem 1. ([6, Proposition 2.1]) *Let n be relatively prime to q and β be a primitive n^{th} root of unity in some extension $\mathbb{E}$ of $\mathbb{F}_q$. Let C be a q-ary cyclic code of length n whose dual's basic zero set is $BZ(C^\perp) = \{\beta^{i_1}, \beta^{i_2}, \ldots, \beta^{i_s}\}$ (i.e. the generator polynomial of $C^\perp$ is $\prod_j m_j(x)$ where $m_j(x) \in \mathbb{F}_q[x]$ is the minimal polynomial of β^{i_j} over $\mathbb{F}_q$). Then we have*

$$C = \left\{ \left(\mathrm{Tr}_{\mathbb{E}/\mathbb{F}_q}(c_1\beta^{ti_1} + \cdots + c_s\beta^{ti_s}) \right)_{0 \le t \le n-1} : c_1, \ldots, c_s \in \mathbb{E} \right\}. \tag{12}$$

2 Results

We use the trace representations in [2, Theorem 4.3] and [5, Theorem 5.1] to obtain the two results presented in this section. In the following, we investigate a q.-c. code whose nonzero constituents are full ambient spaces.

Theorem 2. *Suppose C is a q.-c. code over $\mathbb{F}_q$ of length $m\ell$ and index ℓ of the form*

$$C = \left(G_{i_1}^\ell \oplus \cdots \oplus G_{i_e}^\ell\right) \bigoplus \left((H_{j_1}^{'})^\ell \oplus \cdots \oplus (H_{j_f}^{'})^\ell\right) \bigoplus \left((H_{k_1}^{''})^\ell \oplus \cdots \oplus (H_{k_h}^{''})^\ell\right), \tag{13}$$

where $\{i_1, \ldots, i_e\} \subset \{1, \ldots, s\}$ and $\{j_1, \ldots, j_f\}, \{k_1, \ldots, k_h\} \subset \{1, \ldots, t\}$ (cf. Eqns (10) and (11)). Let $u_{i_1}, \ldots, u_{i_e}, v_{j_1}, \ldots, v_{j_f}, w_{k_1}, \ldots, w_{k_h}$ denote fixed representatives of q-cyclotomic cosets mod m corresponding to the fields appearing

in (13) (i.e. corresponding to the powers of ξ among the roots of g_i, h_j, h_j^*, respectively). Then

$$\dim(C) = \ell \dim(D) \quad \textit{and} \quad d(C) = \ell d(D),$$

where D is the q-ary cyclic code of length m whose dual's basic zero set is

$$BZ(D^{\perp}) = \{\xi^{-u_{i_1}}, \ldots, \xi^{-u_{i_e}}, \xi^{-v_{j_1}}, \ldots, \xi^{-v_{j_f}}, \xi^{-w_{k_1}}, \ldots, \xi^{-w_{k_h}}\}.$$

Recall from Remark 1 that any 2-D cyclic code of size $m \times \ell$ is a q.-c. code of length $m\ell$ and index ℓ. The next result shows that the converse of this statement holds for q.-c. codes with cyclic constituents in (11). Namely, let C be q.-c. of length $m\ell$, index ℓ over $\mathbb{F}_q$ such that

$$C = (C_1 \oplus \cdots \oplus C_e) \bigoplus (D_1 \oplus \cdots \oplus D_f) \bigoplus (E_1 \oplus \cdots \oplus E_h), \tag{14}$$

where $C_a \subset G_{i_a}^{\ell}$ $(1 \le a \le e)$, $D_b \subset (H_{j_b}^{'})^{\ell}$ $(1 \le b \le f)$, $E_d \subset (H_{k_d}^{''})^{\ell}$ $(1 \le d \le h)$ are all cyclic codes of length ℓ over various extensions of $\mathbb{F}_q$. We define these cyclic constituent codes by their duals' basic zero sets:

$$\begin{array}{lll} BZ(C_1^{\perp}) = \left\{\eta^{x_{1,1}}, \ldots, \eta^{x_{1,k_1}}\right\} & BZ(D_1^{\perp}) = \left\{\eta^{y_{1,1}}, \ldots, \eta^{y_{1,m_1}}\right\} & BZ(E_1^{\perp}) = \left\{\eta^{z_{1,1}}, \ldots, \eta^{z_{1,n_1}}\right\} \\ \vdots & \vdots & \vdots \\ BZ(C_e^{\perp}) = \left\{\eta^{x_{e,1}}, \ldots, \eta^{x_{e,k_e}}\right\} & BZ(D_f^{\perp}) = \left\{\eta^{y_{f,1}}, \ldots, \eta^{y_{f,m_f}}\right\} & BZ(E_h^{\perp}) = \left\{\eta^{z_{h,1}}, \ldots, \eta^{z_{h,n_h}}\right\} \end{array} \tag{15}$$

As in Theorem 2, let $u_{i_1}, \ldots, u_{i_e}, v_{j_1}, \ldots, v_{j_f}, w_{k_1}, \ldots, w_{k_h}$ denote fixed representatives of q-cyclotomic cosets mod m corresponding to the fields $G_{i_a}, H_{j_b}^{'}, H_{k_d}^{''}$, respectively. Then we have:

Theorem 3. *Let C be a q.-c. code over $\mathbb{F}_q$ of length $m\ell$ and index ℓ such that*

$$C = (C_1 \oplus \cdots \oplus C_e) \bigoplus (D_1 \oplus \cdots \oplus D_f) \bigoplus (E_1 \oplus \cdots \oplus E_h),$$

where each constituent is a cyclic code of length ℓ over various extensions of $\mathbb{F}_q$. Assume that the cyclic constituents are defined by their duals' basic zero sets as in (15). Then C is a 2-D cyclic code of size $m \times \ell$ over $\mathbb{F}_q$ whose dual's basic zero set is

$$BZ(C^{\perp}) = S_1 \cup \cdots \cup S_e \cup S_1^{'} \cup \cdots \cup S_f^{'} \cup S_1^{''} \cup \cdots \cup S_h^{''},$$

where

$$\begin{array}{ll} S_1 = \left\{(\xi^{-u_1}, \eta^{x_{1,1}}), \ldots, (\xi^{-u_1}, \eta^{x_{1,k_1}})\right\} & S_1^{'} = \left\{(\xi^{-v_1}, \eta^{y_{1,1}}), \ldots, (\xi^{-v_1}, \eta^{y_{1,m_1}})\right\} \\ \vdots & \vdots \\ S_e = \left\{(\xi^{-u_e}, \eta^{x_{e,1}}), \ldots, (\xi^{-u_e}, \eta^{x_{e,k_e}})\right\} & S_f^{'} = \left\{(\xi^{-v_f}, \eta^{y_{f,1}}), \ldots, (\xi^{-v_f}, \eta^{y_{f,m_f}})\right\} \end{array}$$

$$\begin{array}{c} S_1^{''} = \left\{(\xi^{-w_1}, \eta^{z_{1,1}}), \ldots, (\xi^{-w_1}, \eta^{z_{1,n_1}})\right\} \\ \vdots \\ S_h^{''} = \left\{(\xi^{-w_h}, \eta^{z_{h,1}}), \ldots, (\xi^{-w_h}, \eta^{z_{h,n_h}})\right\} \end{array} \tag{16}$$

Remark 2. Note that we have taken both m, ℓ to be relatively prime to q so far. Let us make a further assumption that m and ℓ are also relatively prime to each other. Recall that we can view a 2-D cyclic code C of size $m \times \ell$ as an ideal in the group algebra $\mathbb{F}_q[\mathbb{Z}_m \times \mathbb{Z}_\ell]$. With the new assumption, we have an isomorphism of groups $\mathbb{Z}_m \times \mathbb{Z}_\ell \cong \mathbb{Z}_{m\ell}$. Hence, C can be viewed as an ideal in the group algebra $\mathbb{F}_q[\mathbb{Z}_{m\ell}] \cong \mathbb{F}_q[T]/(T^{m\ell} - 1)$. This ring isomorphism just changes the positions of coefficients since it is induced from an isomorphism of the groups involved. Hence, if we have a q.-c. code C of length $m\ell$, index ℓ such that m, ℓ are both relatively prime to q and also coprime to each other, and if the constituents of C are cyclic codes, then C is equivalent to a usual cyclic code of length $m\ell$. This was observed by Lim in [4]. A special case of this remark (for a binary q.-c. code with cyclic constituents of length 5ℓ, index ℓ with ℓ relatively prime to both 5 and 2) was also observed by Bracco et al in [1].

Remark 3. General weight estimates for 2-D cyclic codes have been obtained in [2] and [3]. Realizing some q.-c. codes as 2-D cyclic codes makes it possible to use these estimates in the context of q.-c. codes.

References

1. A.D. Bracco, A.M. Natividad and P. Solé, "On quintic quasi-cyclic codes", *Disc. Appl. Math.*, vol. 156, pp. 3362-3375, 2008.
2. C. Güneri, "Artin-Schreier curves and weights of two-dimensional cyclic codes", *Finite Fields Appl.*, vol. 10, pp. 481-505, 2004.
3. C. Güneri and F. Özbudak, "Multidimensional cyclic codes and Artin-Schreier type hypersurfaces over finite fields", *Finite Fields Appl.*, vol. 14, pp. 44-58, 2008.
4. C.J. Lim, "Quasi-cyclic codes with cyclic constituent codes", *Finite Fields Appl.*, vol. 13, pp. 516-534, 2007.
5. S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: finite fields", *IEEE Trans. Inform. Theory*, vol. 47, pp. 2751-2760, 2001.
6. J. Wolfmann, "New bounds on cyclic codes from algebraic curves", in: Lecture Notes in Computer Science, vol. 388, pp. 47-62, New York: Springer-Verlag, 1989.