Title	On the algebraic structure of quasi-cyclic codes III : generator theory
Author(s)	Ling, San; Sole, Patrick
Citation	Ling, S., & Solé, P. (2005). On the Algebraic Structure of Quasi-Cyclic Codes III: Generator Theory. IEEE Transactions on Information Theory, 51(7), 2692-2700.
Date	2005
URL	http://hdl.handle.net/10220/9826
Rights	

On the Algebraic Structure of Quasi-Cyclic Codes III: Generator Theory

San Ling and Patrick Solé

***Abstract*—Following Parts I and II, quasi-cyclic codes of given index are studied as codes over a finite polynomial ring. These latter codes are decomposed by the Chinese Remainder Theorem (CRT), or equivalently the Mattson–Solomon transform, into products of shorter codes over larger alphabets. We characterize and enumerate self-dual one-generator quasi-cyclic codes in that context. We give an algorithm to remove some equivalent codes from that enumeration. A generalization to multigenerator codes is sketched.**

***Index Terms*—Automorphism group, Chinese Remainder Theorem (CRT), discrete Fourier transform (DFT), quasi-cyclic codes, self-dual codes.**

I. Introduction

Quasi-cyclic codes have been studied for more than 40 years [2]. Most of the work has concentrated on the so-called one-generator class, the case of a generator matrix consisting of one row of circulants. This class bears striking similarity with cyclic codes, including notions of generator and parity-check polynomials [14], [15]. In a series of recent papers [9], [10], the present authors introduced a spectral approach to quasi-cyclic codes. In that approach, a quasi-cyclic code is decomposed by the Chinese Remainder Theorem (CRT), or equivalently the Mattson–Solomon transform, into products of shorter codes over larger alphabets. The aim of this correspondence is to use the spectral characterization to enumerate and classify one-generator quasi-cyclic codes. These will be further simplified by symmetry considerations. Most of these results will be extended to the multigenerator case.

The material is organized as follows. Basic notions on codes are recalled in Section II, including a brief review of the spectral decomposition of quasi-cyclic codes. In Section III, the spectral approach is applied to one-generator quasi-cyclic codes—characterization and enumeration results are obtained. In Section IV, equivalence of one-generator quasi-cyclic codes is studied. In particular, a certain cyclically shifted multiplier equivalence is characterized, and enumeration of one-generator quasi-cyclic codes up to such equivalence is linked to the enumeration of orbits of certain finite abelian groups under explicit group actions. Examples of such enumeration are given in Section V. Several of the results in Section IV are generalizations of results of [14]. These generalizations are applicable in a wider context with fewer conditions imposed, and the proofs are rather different in nature. In Section VI, some of the results in Section III are extended to the case of multigenerator quasi-cyclic codes with examples given in Section VII. Finally, Section VIII gives some concluding remarks and open problems.

S. Ling was with the Department of Mathematics, National University of Singapore, Singapore 117543, Singapore. He is now with the Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Singapore (e-mail: lingsan@ntu.edu.sg).

P. Solé is with the Centre National de la Recherche Scientifique (CNRS), I3S, ESSI, 06 903 Sophia Antipolis, France (e-mail: ps@essi.fr).

Communicated by C. Carlet, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2005.850142

II. Facts and Notation

A. Codes Over Fields

Let F denote a finite field. When its cardinality q needs to be specified, we will write $F = \boldsymbol{F}_q$. If L is an extension of degree s of F, then the trace of $x \in L$ down to F is

$$Tr_{L/F}(x) := x + x^q + x^{q^2} + \cdots + x^{q^{s-1}}.$$

A linear code of length n over F is an F-vector subspace of F^n. The dual $C^\perp$ of a code C is understood with respect to the standard inner product. A code C is *self-dual* if $C = C^\perp$. We denote by T the standard shift operator on F^n. A (linear) code is said to be *quasi-cyclic* of index ℓ or ℓ-quasi-cyclic if and only if it is invariant under T^ℓ. If $\ell = 1$, it is just a cyclic code. Throughout the correspondence, we shall assume that the index ℓ divides the length n. For instance, if $\ell = 2$ and the first circulant block is the identity matrix, such a code is equivalent to a so-called pure *double circulant* code [11]. More generally, up to equivalence, the generator matrix of such a code consists of $m \times m$ circulant matrices.

B. Codes Over Rings

For a commutative ring A with identity, a linear code C of length n over A is an A submodule of A^n. If C is a subset of A^n, checking linearity is equivalent to checking the following two conditions: 1) x, $y \in C \Longrightarrow x + y \in C$ and 2) $\forall \lambda \in A$, $x \in C \Longrightarrow \lambda x \in C$ with addition and scalar multiplication as per the laws of the ring A.

C. Quasi-Cyclic Codes

Let F be a finite field, and let m be a positive integer coprime with the characteristic of F. Let $F[Y]$ denote the ring of polynomials in the indeterminate Y with coefficients in F. Let $R := R(F, m) = F[Y]/(Y^m - 1)$.

For a positive integer ℓ, define a map $\phi : F^{\ell m} \to R^\ell$ by

$$\phi(\boldsymbol{c}) = (\boldsymbol{c}_0(Y), \boldsymbol{c}_1(Y), \ldots, \boldsymbol{c}_{\ell-1}(Y)) \in R^\ell \tag{1}$$

where $\boldsymbol{c}_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in R$ and

$$\boldsymbol{c} = (c_{00}, c_{01}, \ldots, c_{0,\ell-1}, c_{10}, \ldots, c_{1,\ell-1}, \ldots, c_{m-1,0}, \ldots, c_{m-1,\ell-1}).$$

It is known (cf. [8] and [9], for instance) that ϕ induces a one-to-one correspondence between quasi-cyclic codes over F of index ℓ and length ℓm and linear codes over R of length ℓ. Furthermore, if C is a quasi-cyclic code over F of length ℓm and of index ℓ, then $\phi(C)^\perp = \phi(C^\perp)$, where the dual in $F^{\ell m}$ is taken with respect to the Euclidean inner product, while the dual in R^ℓ is taken with respect to the Hermitian inner product (see [9] for definition). In particular, a quasi-cyclic code C over F is self-dual with respect to the Euclidean inner product if and only if $\phi(C)$ is self-dual over R with respect to the Hermitian inner product.

The polynomial $Y^m - 1$ admits a factorization as follows:

$$Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$$

where δ is nonzero in F, $g_1, \ldots, g_s$ are monic irreducible polynomials that are associates to their own reciprocals, and $h_1, h_1^*, \ldots, h_t, h_t^*$ are pairs of mutually reciprocal monic irreducible polynomials.

Consequently, we may now write

$$R = \frac{F[Y]}{(Y^m-1)} = \left(\bigoplus_{i=1}^{s} \frac{F[Y]}{(g_i)}\right) \oplus \left(\bigoplus_{j=1}^{t} \left(\frac{F[Y]}{(h_j)} \oplus \frac{F[Y]}{(h_j^*)}\right)\right). \quad (2)$$

For simplicity, we denote $F[Y]/(g_i)$ by G_i, $F[Y]/(h_j)$ by H_j', and $F[Y]/(h_j^*)$ by H_j''.

It follows that every R-linear code C of length ℓ can be decomposed as the direct sum

$$C = \left(\bigoplus_{i=1}^{s} C_i\right) \oplus \left(\bigoplus_{j=1}^{t} \left(C_j' \oplus C_j''\right)\right) \quad (3)$$

where, for each $1 \le i \le s$, C_i is a linear code over G_i of length ℓ and, for each $1 \le j \le t$, C_j' is a linear code over H_j' of length ℓ, and C_j'' is a linear code over H_j'' of length ℓ.

The corresponding decomposition of $C^\perp$ is given as [9, Proposition 4.1]

$$C^\perp = \left(\bigoplus_{i=1}^{s} C_i^\perp\right) \oplus \left(\bigoplus_{j=1}^{t} \left((C_j'')^\perp \oplus (C_j')^\perp\right)\right) \quad (4)$$

where $C_i^\perp$ denotes the dual of C_i with respect to the Hermitian inner product (this is the inner product induced by $Y \mapsto Y^{-1}$ [9], not the usual Hermitian inner product) and $(C_j')^\perp$ (resp. $(C_j'')^\perp$) denotes the dual of C_j' (resp. C_j'') with respect to the Euclidean inner product.

The decomposition (4) leads to the following characterization [9, Theorem 4.2] of self-dual codes over R that we will need later.

Theorem 2.1: A linear code C over $R(F,m)$ of length ℓ is self-dual with respect to the Hermitian inner product, or, equivalently, an ℓ-quasi-cyclic code of length ℓm over F is self-dual with respect to the Euclidean inner product if and only if

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

where, for $1 \le i \le s$, C_i is a self-dual code over G_i of length ℓ (with respect to the Hermitian inner product) and, for $1 \le j \le t$, C_j' is a linear code of length ℓ over H_j', and $C_j'^\perp$ is its dual with respect to the Euclidean inner product.

When there is no need to distinguish between the two types of irreducible factors (i.e., self-reciprocal and otherwise) of Y^m-1, instead of (3), we adopt the less cumbersome notation $Y^m - 1 = f_1 \cdots f_r$, where f_i ($1 \le i \le r$) is a monic irreducible polynomial of degree m_i, and

$$C = \bigoplus_{i=1}^{r} C_i \quad (5)$$

where $r = s + 2t$ and C_i is a linear code of length ℓ over $F_i := F[Y]/(f_i)$.

III. One-Generator Codes

A quasi-cyclic code C is one-generator if and only if its generator matrix over the ring R contains only one row, as follows:

$$[a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)].$$

We first recall a few definitions and results from [3], [14], and [15]. The *generator polynomial* of such a code is defined as

$$g(Y) := GCD(a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y), Y^m - 1)$$

and its *parity-check polynomial* as $h(Y) := (Y^m-1)/g(Y)$. If α denotes a primitive m^{th} root of unity in a suitable extension of F, then the *characteristic set* of C is the set of indexes i ($i \in \{1, \ldots, r\}$) such that f_i divides h.

Theorem 3.1: (cf. [3, Corollary 5, Part 3)]) If C is a one-generator ℓ-quasi-cyclic code of length ℓm over F, then it decomposes under the CRT as

$$C = \bigoplus_{i=1}^{r} C_i$$

where C_i is either trivial or an $[\ell, 1]$ code over F_i. Let Z denote the set of indexes i ($i \in \{1, \ldots, r\}$) where C_i is trivial. Then, $g(Y) = \prod_{i \in Z} f_i(Y)$, i.e., $\{1, \ldots, r\} \setminus Z$ is the characteristic set of C, and $\dim(C) = m - \deg(g)$. Conversely, every quasi-cyclic code with all C_i's of dimension at most 1 is a one-generator quasi-cyclic code.

Theorem 3.1 also follows readily from the following observation: Let $\boldsymbol{c} = (a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y))$ be a codeword in C. For each $1 \le i \le r$, let $\gamma_i \in F_i$ denote a root of f_i. Then, the projection of $\boldsymbol{c}$ in C_i is $(a_0(\gamma_i), a_1(\gamma_i), \ldots, a_{\ell-1}(\gamma_i))$.

Theorem 3.1 also leads to the following observations.

Corollary 3.2: Let $\ell \ge 2$ and let C be a one-generator ℓ-quasi-cyclic code with component codes C_i ($1 \le i \le s$) and C_j', C_j'' ($1 \le j \le t$) as in (3). Then, the following statements are equivalent:

i) $C^\perp$ is also a one-generator ℓ-quasi-cyclic code;
ii) $\ell = 2$ and $\dim(C_i) = 1 = \dim(C_j') = \dim(C_j'')$ for all $1 \le i \le s$ and $1 \le j \le t$;
iii) $\ell = 2$ and $h(Y) = Y^m - 1$;
iv) $\ell = 2$ and $\dim(C) = m$.

Proof: Since C is a one-generator quasi-cyclic, it follows that $\dim(C_i) \le 1$ ($1 \le i \le s$) and $\dim(C_j') \le 1$, $\dim(C_j'') \le 1$ ($1 \le j \le t$).

From (4), we see that the component codes of $C^\perp$ are $C_i^\perp$ ($1 \le i \le s$) and $(C_j')^\perp, (C_j'')^\perp$ ($1 \le j \le t$). Statement i) holds if and only if $\ell - \dim(C_i) = \dim(C_i^\perp) \le 1$ ($1 \le i \le s$) and

$$\ell - \dim(C_j') = \dim((C_j')^\perp) \le 1$$
$$\ell - \dim(C_j'') = \dim((C_j'')^\perp) \le 1 \qquad (1 \le j \le t)$$

which is equivalent to $\ell = 2$ and $\dim(C_i) = 1 = \dim(C_j') = \dim(C_j'')$ for all $1 \le i \le s$ and $1 \le j \le t$. The equivalence of ii), iii), and iv) is obvious. □

The self-dual subclass of the preceding is even more constrained.

Theorem 3.3: If C is a self-dual one-generator ℓ-quasi-cyclic code, then $\ell = 2$ and C decomposes under the CRT as

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

where

- the C_i's are self-dual codes of length 2 over G_i, for $i = 1, \ldots, s$
- the C_j''s are arbitrary [2, 1] codes over H_j', for $i = 1, \ldots, t$.

In this case, $h(Y) = Y^m - 1$ and $g(Y) = 1$.

This yields an enumeration result (cf. [15, Corollary 6 and Theorem 7]).

Corollary 3.4: Let q be a prime power such that -1 is a square in $\boldsymbol{F}_q$, and let m be an integer relatively prime to q. Suppose that $Y^m - 1 = \delta g_1 \cdots g_s h_1 h_1^* \cdots h_t h_t^*$ in $\boldsymbol{F}_q[Y]$, where δ is a nonzero element of $\boldsymbol{F}_q$, $g_1, \ldots, g_s, h_1, h_1^*, \ldots, h_t, h_t^*$ are monic irreducible polynomials such that g_i are self-reciprocal, and h_j and h_j^* are reciprocals.

Suppose further that $g_1 = Y - 1$ and, if m is even, $g_2 = Y + 1$. Let the degree of g_i be $2d_i$, and let the degree of h_j (hence also h_j^*) be e_j. Then, the number of distinct self-dual one-generator quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$ is given by

$$\begin{cases} 4\prod_{i=3}^{s}(q^{d_i}+1)\prod_{j=1}^{t}(1+q^{e_j}) & \text{if } m \text{ is even and } q \text{ is odd} \\ 2\prod_{i=2}^{s}(q^{d_i}+1)\prod_{j=1}^{t}(1+q^{e_j}) & \text{if } m \text{ is odd and } q \text{ is odd} \\ \prod_{i=2}^{s}(q^{d_i}+1)\prod_{j=1}^{t}(1+q^{e_j}) & \text{if } m \text{ is odd and } q \text{ is even.} \end{cases}$$

Finally, we observe that, when $q = 2$, there are no Type II (i.e., doubly even self-dual) one-generator quasi-cyclic codes.

Proposition 3.5: When $q = 2$ and m is odd, there are no Type II one-generator quasi-cyclic codes.

Proof: For C, a quasi-cyclic code over $\boldsymbol{F}_2$, let $g_1(Y) = Y - 1$ so that the corresponding component code C_1 is a binary code of length ℓ. Using the inverse discrete Fourier transform, it is easy to see that $\boldsymbol{x} \in C_1$ implies

$$(\underbrace{\boldsymbol{x}, \ldots, \boldsymbol{x}}_{m \text{ times}}) \in C.$$

Since m is odd and all words in C are doubly even, it follows that all words in C_1 are also doubly even. The self-duality of C implies the self-duality of C_1, so C_1 is of Type II. However, the self-duality of C also implies $\ell = 2$, but all Type II binary codes have a length that is a multiple of 8. Hence, no such C_1 (and hence C) exists. □

IV. Automorphism Group

Assume as always that $(q, m) = 1$. We define in this section the notions of multiplier equivalence and cyclically shifted multiplier equivalence. An enumeration result on distinct one-generator quasi-cyclic codes up to cyclically shifted multiplier equivalence, essentially due to Séguin [14], is given an alternative proof. New enumeration results on self-dual one-generator quasi-cyclic codes up to cyclically shifted multiplier equivalence, more general and stronger than those in [14], are also proved.

The map $\sigma_q : x \mapsto x^q$ is a ring isomorphism from R onto itself. It can be extended to R^ℓ componentwise. Since $(q, m) = 1$, the map σ_q induces a permutation of the coefficients of any polynomial in R, so (1) shows that, for any ℓ-quasi-cyclic C over F, $\sigma_q(C)$ is equivalent to C. We shall say that two quasi-cyclic codes C and D over F are *multiplier equivalent* if $\sigma_q^e(C) = D$, for some e.

Proposition 4.1: Two one-generator ℓ-quasi-cyclic codes C and D are multiplier equivalent if and only if the following occurs:

1) they have the same characteristic set K;
2) for each index $i \in K$, the component codes C_i and D_i afford generator matrices

$$[c_0^{(i)}, c_1^{(i)}, \ldots, c_{\ell-1}^{(i)}] \quad \text{and} \quad [d_0^{(i)}, d_1^{(i)}, \ldots, d_{\ell-1}^{(i)}]$$

which satisfy $c_j^{(i)q^e} = d_j^{(i)}$ for some e and all $0 \le j \le \ell - 1$.

Proof: Suppose C and D are multiplier-equivalent one-generator ℓ-quasi-cyclic codes. If C has generator matrix

$$[a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)]$$

then

$$[a_0(Y^{q^e}), a_1(Y^{q^e}), \ldots, a_{\ell-1}(Y^{q^e})]$$

is a generator matrix for $D = \sigma_q^e(C)$.

Let γ_i $(1 \le i \le r)$ be a root of f_i. Then, the component code C_i has as a generator matrix $[a_0(\gamma_i), a_1(\gamma_i), \ldots, a_{\ell-1}(\gamma_i)]$, and D_i has as a generator matrix

$$[a_0(\gamma_i^{q^e}), a_1(\gamma_i^{q^e}), \ldots, a_{\ell-1}(\gamma_i^{q^e})] = [a_0(\gamma_i)^{q^e}, a_1(\gamma_i)^{q^e}, \ldots, a_{\ell-1}(\gamma_i)^{q^e}].$$

Let K_C and K_D denote the characteristic sets of C and D, respectively. Then, $i \in K_C$ if and only if

$$[a_0(\gamma_i), a_1(\gamma_i), \ldots, a_{\ell-1}(\gamma_i)] \neq [0, \ldots, 0].$$

Similarly, $i \in K_D$ if and only if

$$[a_0(\gamma_i)^{q^e}, a_1(\gamma_i)^{q^e}, \ldots, a_{\ell-1}(\gamma_i)^{q^e}] \neq [0, \ldots, 0].$$

Hence, $K_C = K_D$.

Moreover, if $[c_0^{(i)}, c_1^{(i)}, \ldots, c_{\ell-1}^{(i)}]$ and $[d_0^{(i)}, d_1^{(i)}, \ldots, d_{\ell-1}^{(i)}]$ are generator matrices of C_i and D_i, respectively, then there exist nonzero scalars μ_i and ν_i such that $c_j^{(i)} = \mu_i a_j(\gamma_i)$ and $d_j^{(i)} = \nu_i a_j(\gamma_i)^{q^e}$ for all $0 \le j \le \ell - 1$. Hence, $c_j^{(i)q^e} = \lambda_i d_j^{(i)}$ for some $\lambda_i \neq 0$. Finally, we note that $[d_0^{(i)}, d_1^{(i)}, \ldots, d_{\ell-1}^{(i)}]$ is a generator matrix of D_i if and only if so is $[\lambda_i d_0^{(i)}, \lambda_i d_1^{(i)}, \ldots, \lambda_i d_{\ell-1}^{(i)}]$.

Conversely, if $K_C = K_D = K$ and, for every $i \in K$, there exists e (same for all i) such that $c_j^{(i)q^e} = d_j^{(i)}$ for all $0 \le j \le \ell - 1$ (where $[c_0^{(i)}, \ldots, c_{\ell-1}^{(i)}]$ and $[d_0^{(i)}, \ldots, d_{\ell-1}^{(i)}]$ are generator matrices of C_i and D_i, respectively), the CRT then shows that C and D afford generator matrices $[a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)]$ and $[a_0(Y)^{q^e}, a_1(Y)^{q^e}, \ldots, a_{\ell-1}(Y)^{q^e}]$, respectively. This implies that $D = \sigma_q^e(C)$. □

Let S_ℓ denote the group of permutations on $\{0, 1, \ldots, \ell - 1\}$. For any $\tau \in S_\ell$, it is clear that the map

$$[a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)] \mapsto [a_{\tau(0)}(Y), a_{\tau(1)}(Y), \ldots, a_{\tau(\ell-1)}(Y)]$$

also induces an equivalence of ℓ-quasi-cyclic codes over F. Such a map may be composed with the multiplier map above to yield

$$[a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)] \mapsto [a_{\tau(0)}(Y)^{q^e}, a_{\tau(1)}(Y)^{q^e}, \ldots, a_{\tau(\ell-1)}(Y)^{q^e}]$$

which is still an equivalence of quasi-cyclic codes.

In the special case where τ is just the "cyclic shift"

$$[a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)] \mapsto [a_{\ell-1}(Y), a_0(Y), \ldots, a_{\ell-2}(Y)]$$

we shall use σ_q' to denote the composed map

$$\sigma_q' : [a_0(Y), a_1(Y), \ldots, a_{\ell-1}(Y)] \mapsto [a_{\ell-1}(Y)^q, a_0(Y)^q, \ldots, a_{\ell-2}(Y)^q].$$

We say that C and D are cyclically shifted multiplier equivalent if $\sigma_q'^{\,e}(C) = D$ for some e.

There is an analog of Proposition 4.1 for cyclically shifted multiplier equivalence. The proof is similar to that for Proposition 4.1, so we omit it.

Proposition 4.2: Two one-generator ℓ-quasi-cyclic codes C and D are cyclically-shifted multiplier equivalent if and only if the following is true:

1) they have the same characteristic set K;
2) for each index $i \in K$, the component codes C_i and D_i afford generator matrices $[c_0^{(i)}, c_1^{(i)}, \ldots, c_{\ell-1}^{(i)}]$ and $[d_0^{(i)}, d_1^{(i)}, \ldots, d_{\ell-1}^{(i)}]$, which satisfy $c_j^{(i)q^e} = d_{j+e}^{(i)}$ for some e and all $0 \le j \le \ell-1$. (Here, the suffixes $j+e \in \{0, \ldots, \ell-1\}$ are taken modulo ℓ.)

The following enumeration result is essentially due to Séguin [14, Sec. III]. We give an alternative proof here.

Theorem 4.3 (Séguin): Let notation be as above, and let $[r]$ denote $\{1, \ldots, r\}$. Assume that $(q, m) = 1$ and $(\ell, m_i) = 1$ for $i \in [r]$, where m_i denotes the degree of the irreducible factor f_i of $Y^m - 1$ in $\boldsymbol{F}_q[Y]$. Then, the number of distinct one-generator ℓ-quasi-cyclic codes of length ℓm over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence is

$$\sum_{K \subseteq [r]} w(q, K)$$

where $w(q, K)$ stands for the number of orbits of $x \mapsto qx$ on the product of cyclic groups of size $L_i := (q^{\ell m_i} - 1)(q^{m_i} - 1)$ for $i \in K$.

Proof: By Proposition 4.2, it is enough to show that, for given K, $w(q, K)$ is the number of distinct one-generator ℓ-quasi-cyclic codes of length ℓm over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence with characteristic set K.

We note first that the condition $(\ell, m_i) = 1$ means that a basis of $\boldsymbol{F}_{q^\ell}$ as an $\boldsymbol{F}_q$-vector space is also a basis for $\boldsymbol{F}_{q^{\ell m_i}}$ as an $\boldsymbol{F}_{q^{m_i}}$-vector space. In particular, let $\{\lambda_0, \lambda_0^q, \ldots, \lambda_0^{q^{\ell-1}}\}$ denote a normal basis of $\boldsymbol{F}_{q^\ell}$ over $\boldsymbol{F}_q$. It is also a basis of $\boldsymbol{F}_{q^{\ell m_i}}$ over $\boldsymbol{F}_{q^{m_i}}$. For simplicity of notation, we set $Q = q^{m_i}$ and $L = Q^\ell = q^{\ell m_i}$.

We need to parametrize the generator matrices of $[\ell, 1]$ codes over $\boldsymbol{F}_Q$. We can view them, up to permutation, as column vectors of the parity-check matrix of the Hamming code of length L_i over $\boldsymbol{F}_Q$. Denote by Tr the trace from $\boldsymbol{F}_L$ down to $\boldsymbol{F}_Q$. Let β denote a primitive element (i.e., of order $L-1$) in $\boldsymbol{F}_L$. Then we see, by well-known properties of the simplex code, that we can take as generator matrix of an $[\ell, 1]$ code

$$[Tr(\lambda_0\beta^j), Tr(\lambda_0^q\beta^j), \ldots, Tr(\lambda_0^{q^{\ell-1}}\beta^j)], \qquad \text{for } 0 \le j \le L_i - 1.$$

In view of the formula $Tr(z)^q = Tr(z^q)$, valid for all $z \in \boldsymbol{F}_L$, σ_q' acts as $j \mapsto qj$ on the above matrix, i.e.,

$$[Tr(\lambda_0\beta^j), Tr(\lambda_0^q\beta^j), \ldots, Tr(\lambda_0^{q^{\ell-1}}\beta^j)] \mapsto [Tr(\lambda_0\beta^{qj}), Tr(\lambda_0^q\beta^{qj}), \ldots, Tr(\lambda_0^{q^{\ell-1}}\beta^{qj})].$$

Hence, the action of σ_q' is equivalent to that of $x \mapsto qx$ on the product of cyclic groups of order L_i for $i \in K$. □

When $\ell = 2$, σ_q' becomes

$$\sigma_q' : [a_0(Y), a_1(Y)] \mapsto [a_1(Y)^q, a_0(Y)^q].$$

The number of distinct self-dual one-generator two-quasi-cyclic codes up to cyclically shifted multiplier equivalence is linked to the number of orbits of certain explicit group actions, without the conditions $(\ell, m_i) = 1$.

Theorem 4.4: Let q be a prime power such that -1 is a square in $\boldsymbol{F}_q$, and let m be an integer relatively prime to q. Let s, t, d_i, and e_j be as in Corollary 3.4. For every $1 \le j \le t$, let $n_j \in \{2, q^{e_j} - 1\}$, and for $y \in \boldsymbol{Z}_{n_j}$

$$\phi_j(y) = \begin{cases} y + 1, & \text{if } n_j = 2 \\ -qy, & \text{if } n_j = q^{e_j} - 1\,. \end{cases}$$

Then, the number of distinct self-dual one-generator quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence is the sum of the number of orbits under the following group actions (where the n_j and ϕ_j run through all the 2^t possibilities in each case)

i) when q is even

$$(x_2, \ldots, x_s, y_1, \ldots, y_t) \mapsto (-qx_2, \ldots, -qx_s, \phi_1(y_1), \ldots, \phi_t(y_t))$$

on $\boldsymbol{Z}_{q^{d_2}+1} \times \cdots \times \boldsymbol{Z}_{q^{d_s}+1} \times \boldsymbol{Z}_{n_1} \times \cdots \times \boldsymbol{Z}_{n_t}$;

ii) when q is odd and m is odd

$$(x_1, x_2, \ldots, x_s, y_1, \ldots, y_t) \mapsto (x_1 + 1, -\left(qx_2 + \frac{q+1}{2}\right), \ldots, -\left(qx_s + \frac{q+1}{2}\right), \phi_1(y_1), \ldots, \phi_t(y_t))$$

on $\boldsymbol{Z}_2 \times \boldsymbol{Z}_{q^{d_2}+1} \times \cdots \times \boldsymbol{Z}_{q^{d_s}+1} \times \boldsymbol{Z}_{n_1} \times \cdots \times \boldsymbol{Z}_{n_t}$;

iii) when q is odd and m is even

$$(x_1, x_2, x_3, \ldots, x_s, y_1, \ldots, y_t) \mapsto (x_1 + 1, x_2 + 1, -\left(qx_3 + \frac{q+1}{2}\right), \ldots, -\left(qx_s + \frac{q+1}{2}\right), \phi_1(y_1), \ldots, \phi_t(y_t))$$

on $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_{q^{d_3}+1} \times \cdots \times \boldsymbol{Z}_{q^{d_s}+1} \times \boldsymbol{Z}_{n_1} \times \cdots \times \boldsymbol{Z}_{n_t}$.

Proof: We use the same notation as in Corollary 3.4.

Assume first that q is even. Then C_1 has basis $\{(1, \iota)\}$, where $\iota^2 + 1 = 0$, implying that $\iota = 1$. Hence, $C_1 = \langle(1, 1)\rangle$.

For $2 \le i \le s$, the component code C_i is a Hermitian self-dual code of length 2 defined over $\boldsymbol{F}_{q^{2d_i}}$, so $C_i = \langle(1, \lambda)\rangle$ such that $\lambda^{q^{d_i}+1} + 1 = 0$. If ζ_i is a primitive element of $\boldsymbol{F}_{q^{2d_i}}^*$, then it is easy to see that $\lambda \in \langle\zeta_i^{q^{d_i}-1}\rangle$.

For $1 \le j \le t$, the component code C_j' must be a [2, 1] code over $\boldsymbol{F}_{q^{e_j}}$. These are parametrized by (0,1), (1,0) and $(1, \xi_j^i)$, where ξ_j is a primitive element of $\boldsymbol{F}_{q^{e_j}}^*$ and $0 \le i \le q^{e_j} - 2$.

It is now easy to see that σ_q' induces the identity map on C_1 and acts as $\langle(1, \lambda)\rangle \mapsto \left\langle(1, \lambda^{-q})\right\rangle$ on C_i ($2 \le i \le s$). If $C_j' = \langle(1, 0)\rangle$, then $\sigma_q'(C_j') = \langle(0, 1)\rangle$; if $C_j' = \langle(0, 1)\rangle$, then $\sigma_q'(C_j') = \langle(1, 0)\rangle$; and $\sigma_q'(\left\langle(1, \xi_j^i)\right\rangle) = \left\langle(1, \xi_j^{-qi})\right\rangle$. This shows that the action of σ_q' is equivalent to the action in i).

Parts ii) and iii) are proved similarly, except for the following differences.

a) When q is odd, C_1 can be spanned by either $(1, \iota)$ or $(1, -\iota)$, where $\iota^2 + 1 = 0$. Furthermore, if m is even (so $g_1 = Y - 1$ and $g_2 = Y + 1$), then C_2 is also spanned by either $(1, \iota)$ or $(1, -\iota)$. Since $q \equiv 1 \bmod 4$, σ_q' interchanges $\langle(1, \iota)\rangle$ and $\langle(1, -\iota)\rangle$. This explains the action on x_1 in ii) and on x_1, x_2 in iii).
b) When q is odd, the component code C_i ($2 \le i \le s$ if m is odd, and $3 \le i \le s$ if m is even) is parametrized by $(1, \zeta_i^{(2j+1)(q^{d_i}-1)/2})$, where $0 \le j \le q^{d_i}$. It is easy to see that σ_q' sends

$$\left\langle(1, \zeta_i^{(2j+1)(q^{d_i}-1)/2})\right\rangle$$

to

$$\left\langle(1, \zeta_i^{(-2(qj+(q+1)/2)+1)(q^{d_i}-1)/2})\right\rangle$$

TABLE I
SUMMARY OF THE EXAMPLES FOR $3 \leq m \leq 31$

m	s	t	d	Actions	N
3	2	0	2	$x \mapsto -2x = x$ on $\mathbf{Z}_3$	3
5	2	0	4	$x \mapsto -2x = 3x$ on $\mathbf{Z}_5$	2
7	1	1	3	$y \mapsto y+1$ on $\mathbf{Z}_2$ $y \mapsto -2y = 5y$ on $\mathbf{Z}_7$	3
9	3	0	-	$\mathbf{x} \mapsto -2\mathbf{x}$ on $\mathbf{Z}_3 \times \mathbf{Z}_9$	15
13	2	0	12	$x \mapsto -2x$ on $\mathbf{Z}_{65}$	7
15	3	1	-	$(x_1, x_2, y) \mapsto (-2x_1, -2x_2, y+1)$ on $\mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_2$ $(x_1, x_2, y) \mapsto (-2x_1, -2x_2, -2y)$ on $\mathbf{Z}_3 \times \mathbf{Z}_5 \times \mathbf{Z}_{15}$	74
23	1	1	11	$y \mapsto y+1$ on $\mathbf{Z}_2$ $y \mapsto -2y$ on $\mathbf{Z}_{2047}$	95
31	1	3	5	$(y_1, y_2, y_3) \mapsto (y_1+1, y_2+1, y_3+1)$ on $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$ $(y_1, y_2, y_3) \mapsto (y_1+1, y_2+1, -2y_3)$ on $\mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_{31}$ $(y_1, y_2, y_3) \mapsto (y_1+1, -2y_2, y_3+1)$ on $\mathbf{Z}_2 \times \mathbf{Z}_{31} \times \mathbf{Z}_2$ $(y_1, y_2, y_3) \mapsto (-2y_1, y_2+1, y_3+1)$ on $\mathbf{Z}_{31} \times \mathbf{Z}_2 \times \mathbf{Z}_2$ $(y_1, y_2, y_3) \mapsto (y_1+1, -2y_2, -2y_3)$ on $\mathbf{Z}_2 \times \mathbf{Z}_{31} \times \mathbf{Z}_{31}$ $(y_1, y_2, y_3) \mapsto (-2y_1, y_2+1, -2y_3)$ on $\mathbf{Z}_{31} \times \mathbf{Z}_2 \times \mathbf{Z}_{31}$ $(y_1, y_2, y_3) \mapsto (-2y_1, -2y_2, y_3+1)$ on $\mathbf{Z}_{31} \times \mathbf{Z}_{31} \times \mathbf{Z}_2$ $(y_1, y_2, y_3) \mapsto (-2y_1, -2y_2, -2y_3)$ on $\mathbf{Z}_{31} \times \mathbf{Z}_{31} \times \mathbf{Z}_{31}$	3605

so this explains the action on $x_2, \ldots, x_s$ in ii) and $x_3, \ldots, x_s$ in iii). □

Remarks:

i) We have $q^{e_j} - 1 = 2$ if and only if $q = 3$ and $e_j = 1$. However, e_j is always even (cf. [9, Sec. IV, Remark 2]). Thus, $q^{e_j} - 1$ is never 2, and hence there are genuinely 2^t distinct tuples $(n_1, \ldots n_t)$.

ii) Theorem 4.4 is much more general than the results in [14, Sec. IV]. Theorem 4.4 holds for all prime powers q for which self-dual one-generator quasi-cyclic codes exist, while [14, Sec. IV] only deals with the binary case. Furthermore, [14, Sec. IV] assumes that $(2, m_i) = 1$, while this is not needed in Theorem 4.4.

When m is a prime number, Theorem 4.4 actually affords a neater description. We first begin with a lemma.

Lemma 4.5: When m is an odd prime, apart from $Y - 1$, the irreducible factors of $Y^m - 1$ all have the same degree d. Furthermore, either all of these factors are self-reciprocal or none of them is self-reciprocal.

Proof: When m is an odd prime and if $i \not\equiv 0 \bmod m$, we have that $q^e i \equiv i \bmod m$ if and only if $q^e \equiv 1 \bmod m$. This shows that all the q-cyclotomic cosets modulo m, apart from $\{0\}$, have the same size, so the irreducible factors of $Y^m - 1$, except for the factor $Y - 1$, have the same degree.

Similarly, $q^e i \equiv -i \bmod m$ if and only if $q^e \equiv -1 \bmod m$, so either all the irreducible factors (except $Y - 1$) are self-reciprocal, or they must all come in reciprocal pairs. □

Since Lemma 4.5 shows that either $s = 1$ or $t = 0$, Theorem 4.4 has a simpler description when m is an odd prime. (The case $m = 2$ is trivial.)

Corollary 4.6: Let q be a prime power such that -1 is a square in $\boldsymbol{F}_q$, and let m be an odd prime number not dividing q. Let s and t be as in Corollary 3.4, and let d be as in Lemma 4.5. For every $1 \leq j \leq t$, let $n_j \in \{2, q^d - 1\}$, and for $y \in \boldsymbol{Z}_{n_j}$

$$\phi_j(y) = \begin{cases} y+1 & \text{if } n_j = 2 \\ -qy & \text{if } n_j = q^d - 1 \end{cases}.$$

Then, the number of distinct self-dual one-generator quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence is the sum of the number of orbits under the following group actions (where the n_j and ϕ_j run through all the 2^t possibilities in each case):

i) when q is even and all irreducible factors are self-reciprocal

$$\boldsymbol{x} \mapsto -q\boldsymbol{x} \text{ on } \underbrace{\boldsymbol{Z}_{q^{d/2}+1} \times \cdots \times \boldsymbol{Z}_{q^{d/2}+1}}_{s-1}$$

ii) when q is even and all irreducible factors, except $Y - 1$, are not self-reciprocal

$$(y_1, \ldots, y_t) \mapsto (\phi_1(y_1), \ldots, \phi_t(y_t))$$

on $\boldsymbol{Z}_{n_1} \times \cdots \times \boldsymbol{Z}_{n_t}$;

iii) when q is odd and all irreducible factors are self-reciprocal

$$(x_1, x_2, \ldots, x_s) \mapsto \left(x_1 + 1, -\left(qx_2 + \frac{q+1}{2}\right) \ldots, -\left(qx_s + \frac{q+1}{2}\right)\right)$$

on $\boldsymbol{Z}_2 \times \underbrace{\boldsymbol{Z}_{q^{d/2}+1} \times \cdots \times \boldsymbol{Z}_{q^{d/2}+1}}_{s-1}$

iv) when q is odd and all irreducible factors, except $Y - 1$, are not self-reciprocal

$$(x, y_1, \ldots, y_t) \mapsto (x+1, \phi_1(y_1), \ldots, \phi_t(y_t))$$

on $\boldsymbol{Z}_2 \times \boldsymbol{Z}_{n_1} \times \cdots \times \boldsymbol{Z}_{n_t}$.

V. EXAMPLES

In this section, we give some examples for the number of distinct self-dual one-generator quasi-cyclic codes up to cyclically shifted multiplier equivalence. Recall from [9, Proposition 6.1] that q is either even or $q \equiv 1 \bmod 4$.

A. $q = 2$

We summarize the examples for $3 \leq m \leq 31$ in Table I. In the table, m, s, t, and d are as in Section IV. "Actions" refer to the group actions of Theorem 4.4 and Corollary 4.6, while N stands for the number of self-dual one-generator quasi-cyclic codes of length $2m$ up to cyclically shifted multiplier equivalence.

B. $m = 3$

Table II summarizes the results in this case, with same notations as above.

TABLE II
SUMMARY OF THE EXAMPLES FOR $m = 3$

q	s	t	d	Actions	N
2 mod 3	2	0	2	(q even) $x \mapsto -qx = x$ on $\mathbf{Z}_{q+1}$	$q+1$
				(q odd) $(x_1, x_2) \mapsto (x_1 + 1, -(qx_2 + \frac{q+1}{2}))$ on $\mathbf{Z}_2 \times \mathbf{Z}_{q+1}$	$q+1$
1 mod 3	1	1	1	(q even) $y \mapsto y + 1$ on $\mathbf{Z}_2$	$(q/2)+1$
				$y \mapsto -qy = -y$ on $\mathbf{Z}_{q-1}$	
				(q odd) $(x, y) \mapsto (x + 1, y + 1)$ on $\mathbf{Z}_2 \times \mathbf{Z}_2$	$q+1$
				$(x, y) \mapsto (x + 1, -y)$ on $\mathbf{Z}_2 \times \mathbf{Z}_{q-1}$	

C. $m = 4$

Since -1 is a square in $\boldsymbol{F}_q$ (a necessary condition for the existence of self-dual codes of length $2m$), we have $Y^4 - 1 = (Y-1)(Y+1)(Y-i)(Y+i)$, where i is a primitive fourth root of unity. Therefore, $s = 2$ and $t = 1$. By Theorem 4.4, we consider the actions $(x_1, x_2, y) \mapsto (x_1 + 1, x_2 + 1, y + 1)$ on $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_2$ and $(x_1, x_2, y) \mapsto (x_1 + 1, x_2 + 1, -qy)$ on $\boldsymbol{Z}_2 \times \boldsymbol{Z}_2 \times \boldsymbol{Z}_{q-1}$. Both actions are fixed-point-free involutions, so the first action has four orbits of size 2, while the second action has $2(q-1)$ orbits of size 2. Hence, there are $2(q+1)$ self-dual one-generator quasi-cyclic codes of length 8 over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence.

D. $m = 5$

Assume q is such that $Y^4 + Y^3 + Y^2 + Y + 1$ is irreducible in $\boldsymbol{F}_q[Y]$, so $Y^5 - 1 = (Y-1)(Y^4 + Y^3 + Y^2 + Y + 1)$. Therefore, $s = 2$, $t = 0$ and $d = 2$.

1) *When q is even*: By Corollary 4.6, we consider the action $x \mapsto -qx$ on $\boldsymbol{Z}_{q^2+1}$. The only fixed point of this action is $x = 0$: if $-qx = x$, then $(q+1)x = 0$. This implies that the order of x divides both $q + 1$ and $q^2 + 1$, but since q is even, $q + 1$ and $q^2 + 1$ are relatively prime.

   It is also easy to verify that this action has no orbit of size 2 or 3. However, the action $x \mapsto -qx$ has order 4, so there are $q^2/4$ orbits of size 4.

   Hence, there are $(q^2/4) + 1$ self-dual one-generator quasi-cyclic codes of length 10 over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence.
2) *When q is odd*: By Corollary 4.6, we consider the action $(x, y) \mapsto (x + 1, -(qy + \frac{q+1}{2}))$ on $\boldsymbol{Z}_2 \times \boldsymbol{Z}_{q^2+1}$. It is straightforward to verify that this action has two orbits of size 2 (with orbit representatives $(0, \frac{q^2-1}{4})$ and $(1, \frac{q^2-1}{4})$), and all remaining orbits ($(q^2 - 1)/2$ of them) have size 4 each. Hence, there are $\frac{q^2-1}{2} + 2$ self-dual one-generator quasi-cyclic codes of length 10 over $\boldsymbol{F}_q$ up to cyclically shifted multiplier equivalence.

E. Vandermonde Construction ($m \mid q - 1$)

In this case, $Y^m - 1 = (Y-1)(Y-\zeta)(Y-\zeta^2)\cdots(Y-\zeta^{m-1})$, where $\zeta \in \boldsymbol{F}_q$ is a primitive m^{th} root of unity.

1) *When m is odd*: $s = 1$ and $t = (m-1)/2$.
   a) *When q is even*: By Theorem 4.4, we need to consider the actions $\phi : (y_1, \ldots, y_t) \mapsto (\phi_1(y_1), \ldots, \phi_t(y_t))$, where

$$\phi_j(y_j) = \begin{cases} y_j + 1, & \text{if } y_j \in \boldsymbol{Z}_2 \\ -qy_j = -y_j, & \text{if } y_j \in \boldsymbol{Z}_{q-1}. \end{cases}$$

   If there is at least a j such that $n_j = 2$, then ϕ is a fixed-point-free involution, and all orbits have size 2. Hence, for $1 \le i \le t$, if i values of $\{n_1, \ldots, n_t\}$ are 2 and $t - i$ values are $q - 1$, the number of orbits is $2^{i-1}(q-1)^{t-i}$. (For each i, there are $\binom{t}{i}$ such tuples $(n_1, \ldots, n_t)$.) When $(n_1, \ldots, n_t) = (q-1, \ldots, q-1)$, ϕ has one fixed point $(0, \ldots, 0)$ and $\{(q-1)^t - 1\}/2$ orbits of size 2. Since

$$\sum_{i=1}^{t} \binom{t}{i} 2^{i-1}(q-1)^{t-i} + 1 + \frac{(q-1)^t - 1}{2} = \frac{(q+1)^t + 1}{2}$$

   there are $\{(q+1)^{(m-1)/2} + 1\}/2$ self-dual one-generator quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$, obtained via the Vandermonde construction, up to cyclically shifted multiplier equivalence.
   b) *When q is odd*: By Theorem 4.4, we need to consider the actions $\phi : (x, y_1, \ldots, y_t) \mapsto (x+1, \phi_1(y_1), \ldots, \phi_t(y_t))$, with ϕ as in a). Clearly, ϕ is a fixed-point-free involution, and all orbits have size 2. Hence, for $0 \le i \le t$, if i values of $\{n_1, \ldots, n_t\}$ are 2 and $t - i$ values are $q - 1$, the number of orbits is $2^i(q-1)^{t-i}$. (For each i, there are $\binom{t}{i}$ such tuples $(n_1, \ldots, n_t)$.) Since

$$\sum_{i=0}^{t} \binom{t}{i} 2^i (q-1)^{t-i} = (q+1)^t$$

   there are $(q+1)^{(m-1)/2}$ self-dual one-generator quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$, obtained via the Vandermonde construction, up to cyclically shifted multiplier equivalence.
2) *When m is even*: In this case, q is clearly odd, and $s = 2$ and $t = (m-2)/2$. By Theorem 4.4, we need to consider the actions $\phi : (x_1, x_2, y_1, \ldots, y_t) \mapsto (x_1 + 1, x_2 + 1, \phi_1(y_1), \ldots, \phi_t(y_t))$, with ϕ as above. Again, ϕ is clearly a fixed-point-free involution, and all orbits have size 2. Hence, for $0 \le i \le t$, if i values of $\{n_1, \ldots, n_t\}$ are 2 and $t - i$ values are $q - 1$, the number of orbits is $2^{i+1}(q-1)^{t-i}$. (For each i, there are $\binom{t}{i}$ such tuples $(n_1, \ldots, n_t)$.) Since

$$\sum_{i=0}^{t} \binom{t}{i} 2^{i+1}(q-1)^{t-i} = 2(q+1)^t$$

   there are $2(q+1)^{(m-2)/2}$ self-dual one-generator quasi-cyclic codes of length $2m$ over $\boldsymbol{F}_q$, obtained via the Vandermonde construction, up to cyclically shifted multiplier equivalence.

VI. MULTIGENERATOR CASE

In this section, we deal with ρ-generators codes, i.e., quasi-cyclic codes C which afford a generator matrix consisting of ρ rows over the ring $R(F, m) = F[Y]/(Y^m - 1)$. We shall furthermore assume that ρ is the smallest such integer, i.e., C cannot admit any generator matrix with fewer than ρ rows over $R(F, m)$.

With notation as in (5), let k_i denote the dimension of C_i over F_i. Denote by κ (resp. κ') the maximum (resp. minimum) of the k_i for $i = 1, \ldots, r$.

Theorem 6.1: If C is a ρ-generator ℓ-quasi-cyclic code of length ℓm over F, then $\rho = \kappa$. More precisely, C decomposes under the CRT as

$$C = \bigoplus_{i=1}^{r} C_i,$$

where C_i is an $[\ell, k_i]$ code over F_i, with $\rho = \max k_i$. Conversely, every quasi-cyclic code with component codes C_i, of dimension k_i, satisfying $\rho = \max k_i$, is a ρ-generator quasi-cyclic code. Furthermore, in this case, the dimension of C over F is

$$\sum_{i=1}^{r} k_i m_i \leq \rho m.$$

Proof: Suppose C admits a generator matrix whose j^{th} row $\boldsymbol{r}^{(j)}$ $(1 \leq j \leq \rho)$ is given by

$$\boldsymbol{r}^{(j)} = [a_0^{(j)}(Y), a_1^{(j)}(Y), \ldots, a_{\ell-1}^{(j)}(Y)].$$

Let $\gamma_i \in F_i$ denote a root of f_i. Then, clearly C_i is spanned by

$$\boldsymbol{r}_i^{(j)} = [a_0^{(j)}(\gamma_i), a_1^{(j)}(\gamma_i), \ldots, a_{\ell-1}^{(j)}(\gamma_i)], \qquad 1 \leq j \leq \rho.$$

Hence, $k_i \leq \rho$, i.e., $\kappa \leq \rho$.

On the other hand, since $\kappa = \max k_i$, we may suppose that, for each $1 \leq i \leq r$, C_i is spanned by $\boldsymbol{v}_j^{(i)}$ for $1 \leq j \leq \kappa$.

By the CRT, for each $1 \leq j \leq \kappa$, there exists $\boldsymbol{u}_j \in C$ such that

$$\boldsymbol{v}_j^{(i)} = \boldsymbol{u}_j \bmod f_i.$$

The CRT also shows that C is spanned by $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_\kappa$, so $\rho \leq \kappa$. Hence, $\rho = \kappa$.

The final statement on the dimension of C is immediate. □

We are now in a position to enumerate all ρ-generator quasi-cyclic codes.

Corollary 6.2: The number of distinct ρ-generator ℓ-quasi-cyclic codes of length ℓm over F is

$$\prod_{i=1}^{r} \sum_{k_i=0}^{\rho} \begin{bmatrix} \ell \\ k_i \end{bmatrix}_{q^{m_i}} - \prod_{i=1}^{r} \sum_{k_i=0}^{\rho-1} \begin{bmatrix} \ell \\ k_i \end{bmatrix}_{q^{m_i}}$$

where

$$\begin{bmatrix} \ell \\ k_i \end{bmatrix}_{q^{m_i}} = \frac{(q^\ell - 1)(q^\ell - q) \cdots (q^\ell - q^{k_i - 1})}{(q^{k_i} - 1)(q^{k_i} - q) \cdots (q^{k_i} - q^{k_i - 1})}.$$

Proof: The number of C_i of parameters $[\ell, k_i]$ over an extension of degree m_i of F is $\begin{bmatrix} \ell \\ k_i \end{bmatrix}_{q^{m_i}}$ by [11, Ch. 15, Theorem 9]. The result follows. □

Corollary 6.3: Let C be an ℓ-quasi-cyclic code. Then, $C^\perp$ is an $(\ell - \kappa')$-generator ℓ-quasi-cyclic code.

Proof: This follows immediately from the description of the component codes of $C^\perp$ (cf. (4)) and Theorem 6.1. □

Corollary 6.4: Let $\ell \geq 2$, and let C be a ρ-generator ℓ-quasi-cyclic code of length ℓm over F, with component codes C_i $(1 \leq i \leq s)$ and C_j', C_j'' $(1 \leq j \leq t)$ as in (3). If $C^\perp$ is also a ρ-generator ℓ-quasi-cyclic code, then

$$\min\{\dim(C_i), \dim(C_j'), \dim(C_j'') \mid 1 \leq i \leq s, 1 \leq j \leq t\} = \ell - \rho$$

and $\ell \leq 2\rho$.

If $\ell \geq 2\rho$, then the following statements are equivalent:

i) $C^\perp$ is also a ρ-generator ℓ-quasi-cyclic code;
ii) $\ell = 2\rho$ and $\dim(C_i) = \rho = \dim(C_j') = \dim(C_j'')$ for all $1 \leq i \leq s$ and $1 \leq j \leq t$;
iii) $\ell = 2\rho$ and $\dim(C) = \rho m$.

The proof is similar to that for Corollary 3.2.

The self-dual subclass of the preceding is even more constrained.

Theorem 6.5: Let C be a self-dual ρ-generator ℓ-quasi-cyclic code of length ℓm over F. Then, ℓ is even, $\ell \leq 2\rho$, and C decomposes under the CRT as

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

where

- the C_i's are self-dual codes of length ℓ over G_i, for $i = 1, \ldots, s$;
- the C_j''s are arbitrary $[\ell, k_j']$ codes over H_j' with $\ell - \rho \leq k_j' \leq \rho$, for $j = 1, \ldots, t$.

Proof: The theorem follows immediately from Theorem 2.1 and Corollary 6.4. □

Remark: If $t = 0$ (e.g., when $q = 2$ and $m = 3$ or 5), then $\ell = 2\rho$ necessarily in Theorem 6.5.

Theorem 6.5 yields an enumeration result.

Corollary 6.6: Keep notation as in Corollary 3.4. If $\ell > 2\rho$, then there are no self-dual ρ-generator ℓ-quasi-cyclic codes of length ℓm over $\boldsymbol{F}_q$. For $\ell \leq 2\rho$, the number of distinct self-dual ρ-generator ℓ-quasi-cyclic codes of length ℓm over $\boldsymbol{F}_q$ is given by the formulas at the bottom of the page.

Proof: The first two products of the right-hand-side (RHS) of the three formulas follow by [13, p. 184, eqs.(12) and (13)], the last product by [11, Ch. 15, Theorem 9]. □

Proposition 6.7: Let $\ell \leq 2\rho$ be divisible by 8. The number of Type II ρ-generator ℓ-quasi-cyclic codes of length ℓm (m odd) over $\boldsymbol{F}_2$ is

---

$$\left(2 \prod_{i=1}^{\ell/2-1} (q^i + 1)\right)^2 \left(\prod_{i=3}^{s} \prod_{j=0}^{\ell/2-1} (q^{d_i(2j+1)} + 1)\right) \left(\prod_{j=1}^{t} \left(\sum_{k_j'=\ell-\rho}^{\rho} \begin{bmatrix} \ell \\ k_j' \end{bmatrix}_{q^{e_j}}\right)\right), \qquad \text{if } m \text{ is even and } q \text{ is odd}$$

$$\left(2 \prod_{i=1}^{\ell/2-1} (q^i + 1)\right) \left(\prod_{i=2}^{s} \prod_{j=0}^{\ell/2-1} (q^{d_i(2j+1)} + 1)\right) \left(\prod_{j=1}^{t} \left(\sum_{k_j'=\ell-\rho}^{\rho} \begin{bmatrix} \ell \\ k_j' \end{bmatrix}_{q^{e_j}}\right)\right), \qquad \text{if } m \text{ is odd and } q \text{ is odd}$$

$$\left(\prod_{i=1}^{\ell/2-1} (q^i + 1)\right) \left(\prod_{i=2}^{s} \prod_{j=0}^{\ell/2-1} (q^{d_i(2j+1)} + 1)\right) \left(\prod_{j=1}^{t} \left(\sum_{k_j'=\ell-\rho}^{\rho} \begin{bmatrix} \ell \\ k_j' \end{bmatrix}_{q^{e_j}}\right)\right), \qquad \text{if } m \text{ is odd and } q \text{ is even.}$$

found in the first expression at the bottom of the page. For other values of ℓ there are no such codes.

The proof of the first part is similar to that for Proposition 3.5, while that for the last statement is similar to that for Corollary 6.6, using the fact that C is of Type II if and only if its binary component C_1 is of Type II (cf. [6, Theorem 2]).

VII. Examples of Multigenerator Quasi-Cyclic Codes

We exhibit in this section some examples of multigenerator quasi-cyclic codes. In particular, we give the generators in each of these cases.

1) Let $q = 2$ and let $m = 3$. The extended binary Golay code is an eight-quasi-cyclic code of length 24, where the component codes C_1 (over $\boldsymbol{F}_2$) and C_2 (over $\boldsymbol{F}_4$) have generator matrices (cf. [9] and [5])

$$\mathcal{H}_8 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

and

$$\mathcal{H}_8' = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$$

respectively. By the CRT, it is easy to see, therefore, that the extended binary Golay code affords the generator matrix over R, found in the matrix at the bottom of the page.

2) Let $q = 2$ and $m = 5$. In [9], a self-dual binary eight-quasi-cyclic code of parameters [40,20,8] was constructed. In fact, the component codes of this code (over $\boldsymbol{F}_2$ and $\boldsymbol{F}_{16}$, respectively) have generator matrices $\mathcal{H}_8$ and $\mathcal{H}_8'$ also (cf. [9] and [5]). Again, by the CRT, it follows that this code has the following generator matrix over R:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & f(Y) & g(Y) & 1 \\ 0 & 1 & 0 & 0 & g(Y) & 1 & 1 & f(Y) \\ 0 & 0 & 1 & 0 & 1 & 1 & f(Y) & g(Y) \\ 0 & 0 & 0 & 1 & f(Y) & g(Y) & 1 & 1 \end{pmatrix}$$

where

$$f(Y) = Y^4 + Y^3 + Y^2 + Y + 1$$
$$g(Y) = Y^4 + Y^3 + Y^2 + Y$$

3) In [16], the following construction was given. Let q be a power of 2, and let γ be a primitive element of $\boldsymbol{F}_{q^2}$. Let V_e be the $\boldsymbol{F}_q$-span of

$$\{x^{qi+j} + x^{qj+i} : 0 \le i < j \le e-1\} \cup \{x^{(q+1)i} : 0 \le i \le e-1\}.$$

Let

$$C(q,e) = \{(f(1), f(\gamma), \ldots, f(\gamma^{q/2}), f(\gamma^{q+1}), f(\gamma^{q+2}), \ldots, f(\gamma^{(q/2)+q+1}), f(\gamma^{2(q+1)}), \ldots, f(\gamma^{(q-2)(q+1)}), \ldots, f(\gamma^{(q/2)+(q-2)(q+1)})) : f \in V_e\}.$$

It can be seen readily that $C(q,e)$ is quasi-cyclic of index $(q/2)+1$ and is obtained via the Vandermonde construction.

In the case of $C(8,4)$, it is a five-quasi-cyclic code with $m = 7$. (Here, γ is taken to be a root of the irreducible polynomial $x^6 + x^4 + x^3 + x + 1$ over $\boldsymbol{F}_2$.) It is shown in [7] that the component codes C_i ($1 \le i \le 7$) have the following generator matrices ($\mathcal{G}_i$ for C_i):

$$\mathcal{G}_1 = (\,1 \quad 1 \quad 1 \quad 1 \quad 1\,)$$
$$\mathcal{G}_2 = (\,1 \quad \beta^3 \quad \beta^6 \quad \beta^2 \quad \beta^5\,)$$
$$\mathcal{G}_3 = (\,0 \quad \beta^3 \quad \beta^6 \quad \beta^4 \quad \beta^5\,)$$
$$\mathcal{G}_4 = \begin{pmatrix} 0 & \beta^3 & \beta^6 & \beta^5 & \beta^5 \\ 1 & \beta^2 & \beta^4 & \beta^6 & \beta \end{pmatrix}$$
$$\mathcal{G}_5 = \begin{pmatrix} 0 & \beta^5 & \beta^3 & 0 & \beta^6 \\ 0 & \beta^2 & \beta^4 & \beta & \beta \end{pmatrix}$$
$$\mathcal{G}_6 = \begin{pmatrix} 1 & \beta & \beta^2 & \beta^3 & \beta^4 \\ 0 & \beta^2 & \beta^4 & \beta^3 & \beta \end{pmatrix}$$
$$\mathcal{G}_7 = (\,0 \quad \beta \quad \beta^2 \quad \beta^5 \quad \beta^4\,)$$

where $\beta = \gamma^9$ is a root of the irreducible polynomial $x^3 + x + 1$ over $\boldsymbol{F}_2$.

By the CRT again, it can be shown that C has a generator matrix $(a_{ij}(Y))_{1 \le i \le 2, 1 \le j \le 5}$ over R, where

$$a_{11}(Y) = \beta^2 Y^6 + \beta^4 Y^5 + \beta Y^3 + 1$$
$$a_{12}(Y) = \beta^6 Y^6 + \beta^6 Y^5 + \beta^5 Y^4 + \beta Y^3 + \beta Y^2 + \beta^3 Y + \beta^6$$
$$a_{13}(Y) = \beta^2 Y^6 + \beta^5 Y^5 + \beta^2 Y^4 + \beta^5 Y^3 + \beta^6 Y^2 + \beta^3 Y + \beta^5$$
$$a_{14}(Y) = Y^6 + \beta^6 Y^5 + \beta^4 Y^4 + \beta^4 Y^3 + \beta^2 Y^2 + Y$$
$$a_{15}(Y) = \beta^3 Y^6 + \beta^4 Y^5 + \beta^5 Y^4 + \beta^3 Y^3 + \beta^6 Y^2 + \beta^4 Y + \beta^3$$
$$a_{21}(Y) = \beta^3 Y^6 + \beta^6 Y^5 + \beta^2 Y^4 + \beta^5 Y^3 + \beta Y^2 + \beta^4 Y + 1$$
$$a_{22}(Y) = \beta^3 Y^6 + \beta^4 Y^5 + \beta^2 Y^4 + \beta^6 Y^3 + \beta^2 Y^2 + \beta^2 Y + \beta^2$$
$$a_{23}(Y) = \beta^5 Y^6 + \beta^6 Y^5 + \beta^4 Y^4 + \beta Y^3 + \beta^4 Y^2 + \beta^4 Y + \beta^4$$
$$a_{24}(Y) = Y^6 + \beta^4 Y^5 + Y^4 + Y^3 + Y^2 + \beta Y + \beta^2$$
$$a_{25}(Y) = \beta^2 Y^6 + \beta^3 Y^5 + \beta Y^4 + \beta^5 Y^3 + \beta Y^2 + \beta Y + \beta.$$

$$\left(2 \prod_{i=1}^{\ell/2-2} (2^i + 1)\right) \left(\prod_{i=2}^{s} \prod_{j=0}^{\ell/2-1} (2^{d_i(2j+1)} + 1)\right) \left(\prod_{j=1}^{t} \left(\sum_{k_j' = \ell - \rho}^{\rho} \begin{bmatrix} \ell \\ k_j' \end{bmatrix}_{2^{e_j}}\right)\right).$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 1 & Y^2+Y+1 & Y^2+Y & 1 \\ 0 & 1 & 0 & 0 & Y^2+Y & 1 & 1 & Y^2+Y+1 \\ 0 & 0 & 1 & 0 & 1 & 1 & Y^2+Y+1 & Y^2+Y \\ 0 & 0 & 0 & 1 & Y^2+Y+1 & Y^2+Y & 1 & 1 \end{pmatrix}.$$

VIII. Conclusion

In this correspondence, from the characterization of one-generator quasi-cyclic codes under the spectral decomposition, we have studied the enumeration and classification of such codes. A generalization of this result to the multigenerator case is also obtained. A characterization of cyclically shifted multiplier equivalence is also given, which links the enumeration of one-generator quasi-cyclic codes up to such equivalence with the number of orbits of certain explicit group actions.

We end with some open problems to which the results of this correspodence naturally lead. Apart from one-generator quasi-cyclic codes, the class of one-generator quasi-twisted codes has also been studied in the literature (cf. [1] and [4]). Generalizations of the results of this correspondence to this family of codes should be natural. In studying the equivalence of codes in this correspondence, we have restricted ourselves to cyclically shifted multiplier equivalence. As there exist possibly other types of equivalence, it would be natural to see what sort of classification results they would lead to. Finally, some discussion on the multigenerator case has been included in this correspondence, but there certainly is a great deal about this case that remains to be explored.

Acknowledgment

The authors would like to thank B.K. Dey and G. Drolet for sending a copy of [6] and [15], respectively. The authors would also like to thank the anonymous referees for their helpful comments and for pointing out an error in the original draft. P. Solé, who conducted the work in this correspondence while at the National University of Singapore (NUS), Singapore, would like to thank NUS for their kind hospitality.

References

[1] N. Aydin, I. Siap, and D. Ray-Chaudhuri, "The structure of 1-generator quasitwisted codes and new linear codes," *Des. Codes Crypt.*, vol. 24, pp. 313–326, 2001.

[2] Z. Chen.. [Online]. Available: http://www.tec.hkr.se/~chen/research/codes/

[3] J. Conan and G. Séguin, "Structural properties and enumeration of quasi-cyclic codes," *Applicable Algebra in Engineering, Communication and Computing (AAECC)*, vol. 4, pp. 25–39, 1993.

[4] R. Daskalov and P. Hristov, "New quasi-twisted degenerate ternary linear codes," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2259–2263, Sep. 2003.

[5] A. Desideri-Bracco, "Treillis de codes quasicycliques," *Eur. J. Comb.*, vol. 25, pp. 505–516, 2004.

[6] B. K. Dey, "On existence of good self-dual quasicyclic codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1794–1798, Aug. 2004.

[7] Y. S. Kok, "On quasi-cyclic codes," Honors Thesis, Dept. of Mathematics, National University of Singapore, Singapore, 2002.

[8] K. Lally and P. Fitzpatrick, "Algebraic structure of quasicyclic codes," *Disc. Appl. Math.*, vol. 111, pp. 157–175, 2001.

[9] S. Ling and P. Solé, "On the algebraic structure of quasi-cyclic codes I: Finite fields," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 2751–2760, Nov. 2001.

[10] ——, "On the algebraic structure of quasicyclic codes II: Chain rings," *Des. Codes Crypt.*, vol. 30, pp. 113–130, 2003.

[11] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[12] B. R. McDonald, *Finite Rings with Identity*. New York: Marcel Dekker, 1974.

[13] E. Rains and N. J. A. Sloane, "Self-dual codes," in *Handbook of Coding Theory*, W. C. Huffman and V. Pless, Eds. Amsterdam, The Netherlands: North-Holland, 1998.

[14] G. E. Séguin, "A class of 1-generator quasicyclic codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 8, pp. 1745–1753, Aug. 2004.

[15] G. E. Séguin and G. Drolet, "The Theory of 1-Generator Quasi-Cyclic Codes," Dept. Elec. Comp. Eng., Royal Military College , Kingston, ON, Canada, Tech. Rep., 1990.

[16] C. P. Xing and S. Ling, "A class of linear codes with good parameters," *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 2184–2188, Jul. 2000.