On the algebraic structure of quasi-cyclic codes IV : repeated roots

Ling, San; Niederreiter, Harald; Solé, Patrick

2006

Ling, S., Niederreiter, H., & Solé, P. (2006). On the Algebraic Structure of Quasi-cyclic Codes IV: Repeated Roots. *Designs, Codes and Cryptography*, 38(3), 337-361.

<https://hdl.handle.net/10356/96413>

<https://doi.org/10.1007/s10623-005-1431-7>

© 2006 Springer Science+Business Media. This is the author created version of a work that has been peer reviewed and accepted for publication by *Designs, Codes and Cryptography*, Springer Science+Business Media. It incorporates referee's comments but changes resulting from the publishing process, such as copyediting, structural formatting, may not be reflected in this document. The published version is available at:
[<http://dx.doi.org/10.1007/s10623-005-1431-7>].

Downloaded on 26 Apr 2023 20:45:23 SGT

On the Algebraic Structure of Quasi-cyclic Codes IV: Repeated Roots

SAN LING^{*,†}

lingsan@ntu.edu.sg

Division of Mathematical Sciences, School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore 637616, Republic of Singapore

HARALD NIEDERREITER

nied@math.nus.edu.sg

Department of Mathematics, National University of Singapore, Singapore 117543, Republic of Singapore

PATRICK SOLÉ

ps@essi.fr

CNRS, I3S, ESSI, BP 145, Route des Colles, 06 903 Sophia Antipolis, France

Communicated by: T. Helleseth

Abstract. A trace formula for quasi-cyclic codes over rings of characteristic not coprime with the co-index is derived. The main working tool is the Generalized Discrete Fourier Transform (GDFT), which in turn relies on the Hasse derivative of polynomials. A characterization of Type II self-dual quasi-cyclic codes of singly even co-index over finite fields of even characteristic follows. Implications for generator theory are shown. Explicit expressions for the combinatorial duocubic, duoquintic and duoseptic constructions in characteristic two over finite fields are given.

Keywords: quasi-cyclic codes, GDFT, Hasse derivative, codes over rings, self-dual codes, Type II codes

1. Introduction

In a series of papers [17–19], two of the authors laid the foundations of a spectral theory of quasi-cyclic codes. One of the main results was a trace formula analogous to that obtained by employing the Mattson–

^{*}Part of this work was done while the first named author was visiting CNRS-I3S, ESSI, Sophia Antipolis, France. The author would like to thank the institution for the kind hospitality. The research of the first two authors is partially supported by MOE-ARF research Grant R-146-000-029-112 and DSTA research Grant R-394-000-011-422.

[†]Corresponding author.

Solomon polynomial of cyclic codes over finite fields [20]; and one of the main tools in the proof was the Mattson–Solomon polynomial itself, also known as the Discrete Fourier Transform over finite fields. That approach could work only if the characteristic of the field or ring structuring the alphabet was coprime with the co-index.

To relax that condition, a tool already used in the theory of pseudo-random sequences [21], and in the theory of repeated-root cyclic codes is employed in the present work: the Generalized Discrete Fourier Transform (GDFT), which in turn relies on the Hasse derivative of polynomials. As an application some criteria for codes of singly even co-index over finite fields of even characteristic to be Type II are derived (Theorem 7.4, Corollary 8.3).

The material is arranged in the following way. Section 2 collects background material on codes and Hasse derivatives. Section 3 reviews the basic setting of the algebraic theory of quasi-cyclic codes. Section 4 views quasi-cyclic codes as codes over an auxiliary ring depending on the alphabet and the co-index m , and leads naturally to the ring-theoretic development of Section 5. Section 6 is central and culminates with the Trace formula of Theorem 6.2. An application to Type II codes is given in Section 7. Section 8 explores repercussions on generator theory. Section 9 collects some examples of combinatorial constructions and codes constructed from them in characteristic 2 over finite fields.

2. Preliminaries

2.1. Codes

Let q be a prime power and let $\mathbf{F}_q$ denote the finite field of order q .

A linear code of length n over $\mathbf{F}_q$ is an $\mathbf{F}_q$ -vector subspace of $\mathbf{F}_q^n$. 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 $\mathbf{F}_q^n$. 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 paper we shall assume that the index ℓ divides the length n . The quantity $m := n/\ell$ is called the co-index of C . Some basic properties of quasi-cyclic codes have been studied in the literature (cf. [6, 14, 17]).

Codes can also be defined over commutative 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 two conditions

- $x, y \in C \implies x + y \in C$;
- $\forall \lambda \in A, x \in C \implies \lambda x \in C$,

with addition and scalar multiplication as per the laws of the ring A .

2.2. Hasse derivatives

Let $\mathbf{F}_q[Y]$ denote the ring of polynomials in the indeterminate Y with coefficients in $\mathbf{F}_q$.

For a polynomial $g(Y) = \sum_i g_i Y^i$ in $\mathbf{F}_q[Y]$, the j th Hasse derivative (or j th hyperderivative) [13, 15, Section 6.4] is defined as

$$g^{[j]}(Y) = \sum_i \binom{i}{j} g_i Y^{i-j}.$$

Just as in the case of formal derivatives in fields of characteristic 0, Hasse derivatives in any field are related to repeated factors of a polynomial.

PROPOSITION 2.1. [4][15, Lemma 6.51]. *If $f(Y) \in \mathbf{F}_q[Y]$ is irreducible and d is any positive integer, then $f(Y)^d$ divides the polynomial $g(Y)$ if and only if $f(Y)$ divides $g(Y)$ and all its first $d-1$ Hasse derivatives.*

3. Quasi-Cyclic Codes

Let m be a positive integer and let $R := R(q, m) = \mathbf{F}_q[Y]/(Y^m - 1)$.

Let C be a quasi-cyclic code over $\mathbf{F}_q$ of length ℓm and index ℓ . Let

$$\mathbf{c} = (c_{00}, c_{01}, \dots, c_{0,\ell-1}, c_{10}, \dots, c_{1,\ell-1}, \dots, c_{m-1,0}, \dots, c_{m-1,\ell-1})$$

denote a codeword in C .

Define a map $\phi: \mathbf{F}_q^{\ell m} \rightarrow R^\ell$ by

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

where $\mathbf{c}_j(Y) = \sum_{i=0}^{m-1} c_{ij} Y^i \in R$. Let $\phi(C)$ denote the image of C under ϕ . Then we have the following lemma (cf. [17, Lemma 3.1]).

LEMMA 3.1. *The map ϕ induces a one-to-one correspondence between quasi-cyclic codes over $\mathbf{F}_q$ of index ℓ and length ℓm and linear codes over R of length ℓ .*

We define on $\mathbf{F}_q^{\ell m}$ the usual Euclidean inner product: for

$$\mathbf{a} = (a_{00}, a_{01}, \dots, a_{0,\ell-1}, a_{10}, \dots, a_{1,\ell-1}, \dots, a_{m-1,0}, \dots, a_{m-1,\ell-1})$$

and

$$\mathbf{b} = (b_{00}, b_{01}, \dots, b_{0,\ell-1}, b_{10}, \dots, b_{1,\ell-1}, \dots, b_{m-1,0}, \dots, b_{m-1,\ell-1}),$$

we define

$$\mathbf{a} \cdot \mathbf{b} = \sum_{i=0}^{m-1} \sum_{j=0}^{\ell-1} a_{ij} b_{ij}.$$

On R^ℓ , we define the Hermitian inner product: for $\mathbf{x} = (x_0, \dots, x_{\ell-1})$ and $\mathbf{y} = (y_0, \dots, y_{\ell-1})$,

$$\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=0}^{\ell-1} x_j \overline{y_j},$$

where the “conjugation” map $\bar{}$ on R is defined as one that acts as the identity on the elements of $\mathbf{F}_q$ and that sends Y to $Y^{-1} = Y^{m-1}$, and extended $\mathbf{F}_q$ -linearly.

The following results were proved in [17, Proposition 3.2 and Corollary 3.3].

PROPOSITION 3.2. *Let $\mathbf{a}, \mathbf{b} \in \mathbf{F}_q^{\ell m}$. Then $(T^{\ell k}(\mathbf{a})) \cdot \mathbf{b} = 0$ for all $0 \leq k \leq m-1$ if and only if $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$, where T denotes the cyclic shift.*

COROLLARY 3.3. *Let C be a quasi-cyclic code over $\mathbf{F}_q$ of length ℓm and of index ℓ and let $\phi(C)$ be its image in R^ℓ under ϕ . Then $\phi(C)^\perp = \phi(C^\perp)$, where the dual in $\mathbf{F}_q^{\ell m}$ is taken with respect to the Euclidean inner product, while the dual in R^ℓ is taken with respect to the Hermitian inner product. In particular, a quasi-cyclic code C over $\mathbf{F}_q$ 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.*

4. The Ring $R(q, m)$

Let q be a power of a prime p . Let $m = p^a m'$, where $(m', p) = 1$. The polynomial $Y^{m'} - 1$ factors completely into nonassociated irreducible factors in $\mathbf{F}_q[Y]$ as

$$Y^{m'} - 1 = \delta f_1 \cdots f_s f_{s+1} f_{s+1}^* \cdots f_{s+t} f_{s+t}^*,$$

where $\delta \neq 0$ in $\mathbf{F}_q$, $f_1, \dots, f_s$ are irreducible polynomials that are associates to their own reciprocals, and $f_{s+1}, f_{s+1}^*, \dots, f_{s+t}, f_{s+t}^*$ are pairs of mutually reciprocal irreducible polynomials.

Then it follows that, in $\mathbf{F}_q[Y]$, we have

$$\begin{aligned} Y^m - 1 &= Y^{p^a m'} - 1 = (Y^{m'} - 1)^{p^a} \\ &= \delta^{p^a} f_1^{p^a} \cdots f_s^{p^a} f_{s+1}^{p^a} (f_{s+1}^*)^{p^a} \cdots f_{s+t}^{p^a} (f_{s+t}^*)^{p^a}. \end{aligned}$$

Consequently, we may now write

$$R = \frac{\mathbf{F}_q[Y]}{(Y^m - 1)} = \left(\bigoplus_{i=1}^s \frac{\mathbf{F}_q[Y]}{(f_i)^{p^a}} \right) \oplus \left(\bigoplus_{j=1}^t \left(\frac{\mathbf{F}_q[Y]}{(f_{s+j})^{p^a}} \oplus \frac{\mathbf{F}_q[Y]}{(f_{s+j}^*)^{p^a}} \right) \right). \quad (1)$$

The direct sum on the right-hand side is endowed with the coordinatewise addition and multiplication.

For simplicity of notation, whenever m is fixed, we denote $\mathbf{F}_q[Y]/(f_i)^{p^a}$ by R_i , $\mathbf{F}_q[Y]/(f_{s+j})^{p^a}$ by R'_{s+j} and $\mathbf{F}_q[Y]/(f_{s+j}^*)^{p^a}$ by R''_{s+j} . We also denote the fields $\mathbf{F}_q[Y]/(f_i)$ by F_i , $\mathbf{F}_q[Y]/(f_{s+j})$ by F'_{s+j} and $\mathbf{F}_q[Y]/(f_{s+j}^*)$ by F''_{s+j} .

It follows from (1) that

$$R^\ell = \left(\bigoplus_{i=1}^s R_i^\ell \right) \oplus \left(\bigoplus_{j=1}^t (R'_{s+j}{}^\ell \oplus R''_{s+j}{}^\ell) \right).$$

In particular, every R -linear code C of length ℓ can be decomposed as the direct sum

$$C = \left(\bigoplus_{i=1}^s C_i \right) \oplus \left(\bigoplus_{j=1}^t (C'_{s+j} \oplus C''_{s+j}) \right), \quad (2)$$

where, for each $1 \leq i \leq s$, C_i is a linear code over R_i of length ℓ and, for each $1 \leq j \leq t$, C'_{s+j} is a linear code over R'_{s+j} of length ℓ and C''_{s+j} is a linear code over R''_{s+j} of length ℓ .

Every element of R may be written as $\mathbf{c}(Y)$ for some polynomial $\mathbf{c} \in \mathbf{F}_q[Y]$. The decomposition (1) shows that $\mathbf{c}(Y)$ may also be written as an $(s+2t)$ -tuple

$$(c_1(Y), \dots, c_s(Y), c'_{s+1}(Y), c''_{s+1}(Y), \dots, c'_{s+t}(Y), c''_{s+t}(Y)), \quad (3)$$

where $c_i(Y) \in R_i$ ($1 \leq i \leq s$), $c'_{s+j}(Y) \in R'_{s+j}$ and $c''_{s+j}(Y) \in R''_{s+j}$ ($1 \leq j \leq t$). Of course, the c_i , c'_{s+j} and c''_{s+j} may also be considered as polynomials in $\mathbf{F}_q[Y]$.

For any element $\mathbf{r} \in R$, we have earlier defined its “conjugate” $\bar{\mathbf{r}}$, induced by the map $Y \mapsto Y^{-1}$ in R . Suppose that $\mathbf{r}$, expressed in terms of the decomposition (1), is given by

$$\mathbf{r} = (r_1, \dots, r_s, r'_{s+1}, r''_{s+1}, \dots, r'_{s+t}, r''_{s+t}),$$

where $r_i \in R_i$ ($1 \leq i \leq s$), $r'_{s+j} \in R'_{s+j}$ and $r''_{s+j} \in R''_{s+j}$ ($1 \leq j \leq t$). We shall now describe $\bar{\mathbf{r}}$ in terms of the decomposition (1).

We note that, for a polynomial $f \in \mathbf{F}_q[Y]$ that divides $Y^m - 1$, the quotients $\mathbf{F}_q[Y]/(f)$ and $\mathbf{F}_q[Y]/(f^*)$ are isomorphic as rings. The isomorphism is given by

$$\begin{aligned} \frac{\mathbf{F}_q[Y]}{(f)} &\longrightarrow \frac{\mathbf{F}_q[Y]}{(f^*)}, \\ c(Y) + (f) &\longmapsto c(Y^{-1}) + (f^*). \end{aligned} \tag{4}$$

(Here, the symbol Y^{-1} makes sense. It can in fact be considered as Y^{m-1} , since f and hence f^* divide $Y^m - 1$ implies that $Y^m = 1$ in both of these rings.)

In the case where f and f^* are associates, we see from (4) that the map $Y \mapsto Y^{-1}$ induces an automorphism of $\mathbf{F}_q[Y]/(f)$. For $r \in \mathbf{F}_q[Y]/(f)$, we denote by $\bar{r}$ its image under this induced map. When the degree of f is 1, note that the induced map is the identity map, so $\bar{r} = r$.

Therefore, the element $\bar{\mathbf{r}}$ can now be expressed as

$$(\bar{r}_1, \dots, \bar{r}_s, r'_{s+1}, r''_{s+1}, \dots, r'_{s+t}, r''_{s+t}).$$

When f and f^* are associates, for vectors $\mathbf{c} = (c_1, \dots, c_\ell)$, $\mathbf{c}' = (c'_1, \dots, c'_\ell) \in (\mathbf{F}_q[Y]/(f))^\ell$, we define the Hermitian inner product on $(\mathbf{F}_q[Y]/(f))^\ell$ to be

$$\langle \mathbf{c}, \mathbf{c}' \rangle = \sum_{i=1}^{\ell} c_i \bar{c}'_i. \tag{5}$$

The following proposition is now an immediate consequence of the above discussion.

PROPOSITION 4.1. *Let $\mathbf{a}, \mathbf{b} \in R^\ell$ and write*

$$\mathbf{a} = (\mathbf{a}_0, \mathbf{a}_1, \dots, \mathbf{a}_{\ell-1})$$

and

$$\mathbf{b} = (\mathbf{b}_0, \mathbf{b}_1, \dots, \mathbf{b}_{\ell-1}).$$

Decomposing each $\mathbf{a}_i, \mathbf{b}_i$ using (3), we write

$$\mathbf{a}_i = (a_{i1}, \dots, a_{is}, a'_{i1}, a''_{i1}, \dots, a'_{it}, a''_{it})$$

and

$$\mathbf{b}_i = (b_{i1}, \dots, b_{is}, b'_{i1}, b''_{i1}, \dots, b'_{it}, b''_{it}),$$

where $a_{ij}, b_{ij} \in R_j$, $a'_{ij}, b'_{ij}, a''_{ij}, b''_{ij} \in R'_{s+j}$ (with R'_{s+j} and R''_{s+j} identified). Then

$$\begin{aligned} \langle \mathbf{a}, \mathbf{b} \rangle &= \sum_{i=0}^{\ell-1} \mathbf{a}_i \overline{\mathbf{b}_i} \\ &= \left(\sum_i a_{i1} \overline{b_{i1}}, \dots, \sum_i a_{is} \overline{b_{is}}, \sum_i a'_{i1} \overline{b'_{i1}}, \sum_i a''_{i1} \overline{b''_{i1}}, \dots, \right. \\ &\quad \left. \sum_i a'_{it} \overline{b'_{it}}, \sum_i a''_{it} \overline{b''_{it}} \right). \end{aligned}$$

In particular, $\langle \mathbf{a}, \mathbf{b} \rangle = 0$ if and only if $\sum_i a_{ij} \overline{b_{ij}} = 0$ ($1 \leq j \leq s$) and $\sum_i a'_{ik} \overline{b'_{ik}} = 0 = \sum_i a''_{ik} \overline{b''_{ik}}$ ($1 \leq k \leq t$).

An immediate consequence is the following characterization of self-dual codes over R :

THEOREM 4.2. *A linear code C over $R = \mathbf{F}_q[Y]/(Y^m - 1)$ of length ℓ is self-dual with respect to the Hermitian inner product (or equivalently, an ℓ -quasi-cyclic code of length ℓm over $\mathbf{F}_q$ is self-dual with respect to the Euclidean inner product) if and only if*

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

where, for $1 \leq i \leq s$, C_i is a self-dual code over R_i of length ℓ (with respect to the Hermitian inner product) and, for $1 \leq j \leq t$, C'_{s+j} is a linear code of length ℓ over R'_{s+j} and $(C'_{s+j})^\perp$ is its dual with respect to the Euclidean inner product.

5. Finite Chain Rings

The rings R_i , R'_{s+j} and R''_{s+j} in Section 4 are actually finite chain rings [22]. If f is a monic irreducible factor of degree d of $Y^{m'} - 1$, then the quotient ring $\mathbf{F}_q[Y]/(f)^{p^a}$ can be identified with the finite chain ring $\mathbf{F}_{q^d} + u\mathbf{F}_{q^d} + \dots + u^{p^a-1}\mathbf{F}_{q^d}$, where $u^{p^a} = 0$. Let $\mathbf{F}_q[Y]/(f) \simeq \mathbf{F}_{q^d}$ and let $\xi \in \mathbf{F}_{q^d}^*$ be a root of f . The identification of the chain rings is given by the following map:

$$\begin{aligned} \frac{\mathbf{F}_q[Y]}{(f)^{p^a}} &\longrightarrow \mathbf{F}_{q^d} + u\mathbf{F}_{q^d} + \cdots + u^{p^a-1}\mathbf{F}_{q^d}, \\ Y &\longmapsto \xi(1-u). \end{aligned} \quad (6)$$

This map is well defined, as it is easy to verify that $f(Y)^{p^a}$ is mapped to 0 on the right-hand side. Moreover, there exists α such that $\xi^{p^a\alpha} = \xi$, so it follows that $1 - Y^{1-p^a\alpha}$ is mapped to u . Here, the exponent $1 - p^a\alpha$ of Y , taken modulo m , can be regarded as a nonnegative integer, so that $1 - Y^{1-p^a\alpha}$ is indeed a polynomial. Hence, the above map is a ring isomorphism.

The ring on the right-hand side of (6) affords a Frobenius map given by

$$x_0 + ux_1 + \cdots + u^{p^a-1}x_{p^a-1} \mapsto x_0^q + ux_1^q + \cdots + u^{p^a-1}x_{p^a-1}^q.$$

The trace on this ring is given by

$$\begin{aligned} Tr : \mathbf{F}_{q^d} + u\mathbf{F}_{q^d} + \cdots + u^{p^a-1}\mathbf{F}_{q^d} &\longrightarrow \mathbf{F}_q + u\mathbf{F}_q + \cdots + u^{p^a-1}\mathbf{F}_q \\ x_0 + ux_1 + \cdots + u^{p^a-1}x_{p^a-1} &\longmapsto Tr(x_0) + uTr(x_1) + \cdots \\ &\quad + u^{p^a-1}Tr(x_{p^a-1}), \end{aligned}$$

where $Tr : \mathbf{F}_{q^d} \rightarrow \mathbf{F}_q$ is the usual trace map on $\mathbf{F}_{q^d}$ down to $\mathbf{F}_q$.

The fields F_i, F'_{s+j} and F''_{s+j} were introduced in Section 4. These are extensions of $\mathbf{F}_q$. We will denote by Tr_i, Tr'_{s+j} and Tr''_{s+j} the respective traces from these fields down to $\mathbf{F}_q$. These notations will be useful in Theorem 6.2.

6. Trace Description

6.1. Generalized Discrete Fourier Transform

We continue to let $m = p^a m'$, where $(m', p) = 1$. When $a \geq 1$, m is no longer relatively prime to p , so the classical theory of discrete Fourier transform does not apply to $\mathbf{F}_q[Y]/(Y^m - 1)$. However, a generalized discrete Fourier transform has been introduced in the literature (see, e.g., [21]) that deals with this situation.

Let $\mathbf{c} = \sum_{i \in \mathbf{Z}/m\mathbf{Z}} c_i Y^i \in \mathbf{F}_q[Y]/(Y^m - 1)$, and let ζ be a primitive m' th root of 1 in some (sufficiently large) extension of $\mathbf{F}_q$. For each $0 \leq g \leq p^a - 1$ and $0 \leq h \leq m' - 1$, let

$$\hat{c}_{g,h} = \sum_{i \in \mathbf{Z}/m\mathbf{Z}} \binom{i}{g} c_i (\zeta^h)^{i-g}.$$

Then, the generalized discrete Fourier transform of $\mathbf{c}$ can be described in terms of a matrix

$$\hat{\mathbf{c}} = \begin{pmatrix} \hat{c}_{0,0} & \hat{c}_{0,1} & \cdots & \hat{c}_{0,m'-1} \\ \hat{c}_{1,0} & \hat{c}_{1,1} & \cdots & \hat{c}_{1,m'-1} \\ \vdots & & & \\ \hat{c}_{p^a-1,0} & \hat{c}_{p^a-1,1} & \cdots & \hat{c}_{p^a-1,m'-1} \end{pmatrix}.$$

It is easy to see that $\hat{c}_{g,qh} = (\hat{c}_{g,h})^q$.

There is a one-to-one correspondence between the irreducible factors of $Y^{m'} - 1$ and the q -cyclotomic cosets of $\mathbf{Z}/m'\mathbf{Z}$. Let Z_i ($1 \leq i \leq s$), Z'_{s+j} and Z''_{s+j} ($1 \leq j \leq t$) denote the distinct q -cyclotomic cosets corresponding to f_i , f'_{s+j} and f''_{s+j} , respectively. Then the entries of the above matrix can be interpreted as elements of the rings on the right-hand side of (1) as follows: if $h \in Z_i$ (resp. Z'_{s+j} and Z''_{s+j}), then the h th column of the matrix corresponds to the element $\hat{c}_{0,h} + u\hat{c}_{1,h} + u^2\hat{c}_{2,h} + \cdots + u^{p^a-1}\hat{c}_{p^a-1,h}$ of the chain ring $\mathbf{F}_q[Y]/(f_i)^{p^a}$ (resp. $\mathbf{F}_q[Y]/(f'_{s+j})^{p^a}$ and $\mathbf{F}_q[Y]/(f''_{s+j})^{p^a}$). Note that the qh th column of the matrix then corresponds to the element $\hat{c}_{0,h}^q + u\hat{c}_{1,h}^q + u^2\hat{c}_{2,h}^q + \cdots + u^{p^a-1}\hat{c}_{p^a-1,h}^q$.

In fact, the generalized discrete Fourier Transform gives rise to the isomorphism (1). The inverse is given by the inverse transform, whose description is somewhat more involved than that of the classical discrete Fourier Transform. As an explicit description of the inverse transform is necessary for obtaining a trace description of repeated-root quasi-cyclic codes, we recall some details of the inverse transform here.

For each $0 \leq i \leq p^a - 1$, let

$$\mathbf{c}_{(i)}(Y) = c_i + c_{i+p^a}Y + \cdots + c_{i+(m'-1)p^a}Y^{m'-1}.$$

Let $\beta = \zeta^{p^a}$, so that β is again a primitive m' th root of 1. By the classical discrete Fourier transform (with β as the chosen primitive m' th root of 1), one sees readily that

$$c_{i+jp^a} = \frac{1}{m'} \sum_{h=0}^{m'-1} \mathbf{c}_{(i)}(\beta^h)(\beta^{-j})^h.$$

Let $H(Y)$ be the $p^a \times p^a$ matrix whose (i, j) th entry is $\binom{j}{i} Y^{j-i}$, where the rows and columns are labelled from 0 to $p^a - 1$ (this is the i th Hasse derivative of the monomial Y^j in $\mathbf{F}_q[Y]$). It is known that the inverse of $H(Y)$ is $H(-Y)$ (cf. [21, Lemma 6]). In particular, when q is even, $H(Y)$ is self-inverse. It can then be verified (cf. [21, Eq. (4)]) that

$$\begin{pmatrix} \mathbf{c}_{(0)}(\beta^h) \\ \mathbf{c}_{(1)}(\beta^h) \\ \vdots \\ \mathbf{c}_{(p^a-1)}(\beta^h) \end{pmatrix} = H(-\zeta^h) \begin{pmatrix} \hat{c}_{0,h} \\ \hat{c}_{1,h} \\ \vdots \\ \hat{c}_{p^a-1,h} \end{pmatrix}.$$

Consequently,

$$c_{i+jp^a} = \frac{1}{m'} \sum_{h=0}^{m'-1} \left(\sum_{g=0}^{p^a-1} \binom{g}{i} (-\zeta^h)^{g-i} \hat{c}_{g,h} \right) (\beta^{-j})^h.$$

Interchanging the sums and grouping terms from the same cyclotomic coset together, we obtain:

$$\begin{aligned} c_{i+jp^a} &= \frac{1}{m'} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \left(\sum_{h=0}^{m'-1} (\zeta^{g-i})^h \hat{c}_{g,h} (\beta^{-j})^h \right) \\ &= \frac{1}{m'} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \left(\sum_z \text{Tr}(\hat{c}_{g,z} (\zeta^{g-i})^z (\beta^{-j})^z) \right) \\ &= \frac{1}{m'} \sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \left(\sum_z \text{Tr}(\hat{c}_{g,z} \zeta^{(g-i-p^a j)z}) \right), \end{aligned}$$

where the sums over z are taken over all the distinct cyclotomic coset representatives, and Tr denotes the trace from the respective fields down to $\mathbb{F}_q$. Hence the generalized discrete Fourier transform is invertible.

EXAMPLE 6.1. (i) When $p^a = 1$, i.e., $a = 0$, setting $i = 0$, we obtain

$$c_j = \frac{1}{m} \sum_{h=0}^{m-1} \hat{c}_{0,h} (\zeta^{-j})^h,$$

which is the same as the classical discrete Fourier transform since $\hat{c}_{0,h} = c(\zeta^h)$.

(ii) When q is even and $p^a = 2$, we obtain, for $0 \leq j \leq m'$,

$$c_{2j} = \sum_z \text{Tr}(\hat{c}_{0,z} \zeta^{-2jz}) + \sum_z \text{Tr}(\hat{c}_{1,z} \zeta^{(1-2j)z}),$$

and

$$c_{1+2j} = \sum_z \text{Tr}(\hat{c}_{1,z} \zeta^{-2jz}),$$

where z runs through the distinct cyclotomic coset representatives.

As in [17,18], the following characterization result on repeated-root quasi-cyclic codes over $\mathbf{F}_q$ is now obtained.

THEOREM 6.2. *Let $m = p^a m'$ with $(m', p) = 1$, where p is the characteristic of $\mathbf{F}_q$. Then, for any ℓ , the quasi-cyclic codes over $\mathbf{F}_q$ of length ℓm and of index ℓ are precisely given by the following construction: write $Y^{m'} - 1 = \delta f_1 \cdots f_s f_{s+1} f_{s+1}^* \cdots f_{s+t} f_{s+t}^*$, where δ is a nonzero element of $\mathbf{F}_q$, f_i are irreducible factors that are associates to their own reciprocals, and f_{s+j} are irreducible factors whose reciprocals are f_{s+j}^* . Write $\mathbf{F}_q[Y]/(f_i)^{p^a} = R_i$, $\mathbf{F}_q[Y]/(f_{s+j})^{p^a} = R'_{s+j}$ and $\mathbf{F}_q[Y]/(f_{s+j}^*)^{p^a} = R''_{s+j}$. Let Z_i (resp. Z'_{s+j} and Z''_{s+j}) denote the q -cyclotomic coset of $\mathbf{Z}/m'\mathbf{Z}$ corresponding to f_i (resp. f_{s+j} and f_{s+j}^*) and fix $z_i \in Z_i$, $z'_{s+j} \in Z'_{s+j}$ and $z''_{s+j} \in Z''_{s+j}$. For each $1 \leq i \leq s$, let C_i be a code of length ℓ over R_i , and for each $1 \leq j \leq t$, let C'_{s+j} be a code of length ℓ over R'_{s+j} and let C''_{s+j} be a code of length ℓ over R''_{s+j} . For $\mathbf{x}_i \in C_i$, $\mathbf{y}'_j \in C'_{s+j}$ and $\mathbf{y}''_j \in C''_{s+j}$, write*

$$\mathbf{x}_i = \mathbf{x}_{0,i} + u\mathbf{x}_{1,i} + \cdots + u^{p^a-1}\mathbf{x}_{p^a-1,i},$$

$$\mathbf{y}'_j = \mathbf{y}'_{0,j} + u\mathbf{y}'_{1,j} + \cdots + u^{p^a-1}\mathbf{y}'_{p^a-1,j},$$

and

$$\mathbf{y}''_j = \mathbf{y}''_{0,j} + u\mathbf{y}''_{1,j} + \cdots + u^{p^a-1}\mathbf{y}''_{p^a-1,j},$$

where the vectors $\mathbf{x}_{g,i}$, $\mathbf{y}'_{g,j}$ and $\mathbf{y}''_{g,j}$ are in $\mathbf{F}_q^\ell$ ($0 \leq g \leq p^a - 1$).

For each $0 \leq i \leq p^a - 1$ and $0 \leq j \leq m' - 1$, let

$$\begin{aligned} \mathbf{c}_{i+jp^a} = & \frac{1}{m'} \left(\sum_{g=0}^{p^a-1} \binom{g}{i} (-1)^{g-i} \left(\sum_{\gamma=1}^s \text{Tr}_\gamma(\mathbf{x}_{g,z_\gamma} \zeta^{(g-i-p^a j)z_\gamma}) \right. \right. \\ & \left. \left. + \sum_{\delta=s+1}^{s+t} (\text{Tr}'_\delta(\mathbf{y}'_{g,z'_\delta} \zeta^{(g-i-p^a j)z'_\delta}) + \text{Tr}''_\delta(\mathbf{y}''_{g,z''_\delta} \zeta^{(g-i-jp^a)z''_\delta})) \right) \right). \end{aligned}$$

Then the code

$$C = \{(\mathbf{c}_0, \dots, \mathbf{c}_{m-1}) \mid \mathbf{x}_i \in C_i, \mathbf{y}'_j \in C'_{s+j} \text{ and } \mathbf{y}''_j \in C''_{s+j}\}$$

is a quasi-cyclic code over $\mathbf{F}_q$ of length ℓm and of index ℓ . Conversely, every quasi-cyclic code over $\mathbf{F}_q$ of length ℓm and of index ℓ is obtained through this construction. Moreover, C is self-dual if and only if the C_i are self-dual with respect to the Hermitian inner product and $C''_{s+j} = (C'_{s+j})^\perp$ for each j with respect to the Euclidean inner product.

Remark. In the definition of $\mathbf{c}_{i+jp^a}$ in Theorem 6.2, the m' has been suppressed. Note that m' is a unit in $\mathbf{F}_q$, so $m'C = C$.

Consider now the special case where $m' = 1$ and $p^a = 2$ (so q is even and $m = 2$). We obtain the following observation:

COROLLARY 6.3. *Let q be even and let $m = 2$. Then we have an isomorphism*

$$\begin{aligned} \mathbf{F}_q^{2\ell} &\simeq (\mathbf{F}_q + u\mathbf{F}_q)^\ell, \\ (\mathbf{y} + \mathbf{x}, \mathbf{y}) &\leftrightarrow \mathbf{x} + u\mathbf{y}. \end{aligned}$$

The isomorphism in Corollary 6.3 is precisely the usual Gray map on $(\mathbf{F}_q + u\mathbf{F}_q)^\ell$. Therefore, for general prime powers q , the special case of Theorem 6.2 when $m' = 1$ may be a reasonable way to define the Gray map on $\mathbf{F}_q + u\mathbf{F}_q + \cdots + u^{p^a-1}\mathbf{F}_q$.

7. Type II Codes

In the case where $p^a = 1$, it has been shown that an ℓ -quasi-cyclic code of length ℓm over $\mathbf{F}_2$ is of Type II if and only if its binary component (i.e., the component corresponding to the factor $Y - 1$) is of Type II (cf. [7, Theorem 2]). In this section, we extend this result to quasi-cyclic codes over $\mathbf{F}_{2^r}$ when $p^a = 1$ or 2.

First, we recall some notions on codes over $\mathbf{F}_{2^r}$ and $\mathbf{F}_{2^r} + u\mathbf{F}_{2^r}$ cf. [1–3, 8, 16].

It is well known that $\mathbf{F}_{2^r}$ admits a self-dual (or self-complementary) trace-orthogonal basis (TOB), say $B = \{b_1, \dots, b_r\}$, over $\mathbf{F}_2$ [15, p. 75]. Then $Tr(b_i b_j) = \delta_{ij}$, where Tr denotes the trace from $\mathbf{F}_{2^r}$ down to $\mathbf{F}_2$ and δ_{ij} is the Kronecker delta function. Every element $x \in \mathbf{F}_{2^r}$ can be written uniquely as $x = \sum_{i=1}^r x_i b_i$, with $x_i \in \{0, 1\}$. The Lee weight $\text{wt}_L^B(x)$ of x with respect to B is defined as the rational sum $\sum_{i=1}^r x_i$. The Lee weight of a vector over $\mathbf{F}_{2^r}$ is the sum of the Lee weights of its components. A self-dual code over $\mathbf{F}_{2^r}$ is said to be of Type II if and only if the Lee weight of every codeword is a multiple of 4 [2]. This definition is shown in [2] to be independent of the choice of the TOB.

As mentioned earlier, there is a Gray map from $(\mathbf{F}_{2^r} + u\mathbf{F}_{2^r})^\ell$ to $\mathbf{F}_{2^r}^{2\ell}$ given by

$$\begin{aligned} (\mathbf{F}_{2^r} + u\mathbf{F}_{2^r})^\ell &\longrightarrow \mathbf{F}_{2^r}^{2\ell}, \\ \mathbf{x} + u\mathbf{y} &\longmapsto (\mathbf{x} + \mathbf{y}, \mathbf{y}). \end{aligned}$$

With a fixed self-dual TOB B for $\mathbf{F}_{2^r}$, the Lee weight of $\mathbf{x} + u\mathbf{y} \in (\mathbf{F}_{2^r} + u\mathbf{F}_{2^r})^\ell$ with respect to B is defined to be the Lee weight of its Gray

image. A self-dual code over $\mathbf{F}_{2^r} + u\mathbf{F}_{2^r}$ is of Type II if and only if the Lee weight of every codeword is a multiple of 4 [3].

LEMMA 7.1. *Let $\mathbf{x} = (x_1, \dots, x_\ell)$, $\mathbf{y} = (y_1, \dots, y_\ell) \in \mathbf{F}_{2^r}^\ell$ and let B be a self-dual TOB for $\mathbf{F}_{2^r}$ with respect to $\mathbf{F}_2$. Let wt_L^B denote the Lee weight with respect to B . Then*

$$\text{wt}_L^B(\mathbf{x} + \mathbf{y}) \equiv \text{wt}_L^B(\mathbf{x}) + \text{wt}_L^B(\mathbf{y}) - 2\text{wt}_L^B(\mathbf{x} \star \mathbf{y}) \pmod{4},$$

where $\mathbf{x} \star \mathbf{y} = (x_1 y_1, \dots, x_\ell y_\ell)$.

Moreover, if $\mathbf{x} \cdot \mathbf{y} = 0$, then $\text{wt}_L^B(\mathbf{x} \star \mathbf{y}) \equiv 0 \pmod{2}$, so

$$\text{wt}_L^B(\mathbf{x} + \mathbf{y}) \equiv \text{wt}_L^B(\mathbf{x}) + \text{wt}_L^B(\mathbf{y}) \pmod{4}.$$

Proof. Suppose, for all $1 \leq i \leq \ell$, that $x_i = \sum_{j=1}^r x_{ij} b_j$ and $y_i = \sum_{k=1}^r y_{ik} b_k$, where $x_{ij}, y_{ik} \in \{0, 1\}$. Then

$$\text{wt}_L^B(\mathbf{x}) = \sum_{i,j} x_{ij},$$

and

$$\text{wt}_L^B(\mathbf{y}) = \sum_{i,k} y_{ik}.$$

It is easy to check that $\mathbf{x} + \mathbf{y} = (x_1 + y_1, \dots, x_\ell + y_\ell)$, where

$$x_i + y_i = \sum_j (x_{ij} \oplus y_{ij}) b_j,$$

where $\oplus$ denotes the addition in $\mathbf{F}_2$.

Consequently,

$$\text{wt}_L^B(\mathbf{x} + \mathbf{y}) = \sum_{i,j} (x_{ij} + y_{ij} - 2x_{ij}y_{ij}),$$

regarding $x_{ij}, y_{ij} \in \{0, 1\}$.

Writing $b_j b_k = \sum_\lambda \gamma_\lambda^{(j,k)} b_\lambda$, we see readily that

$$\text{wt}_L^B(\mathbf{x} \star \mathbf{y}) = \sum_{i,j,k,\lambda} x_{ij} y_{ik} \gamma_\lambda^{(j,k)}.$$

Since $\text{Tr}(b_i) = \text{Tr}(b_i^2) = 1$, it follows that

$$\sum_\lambda \gamma_\lambda^{(j,k)} = \delta_{jk},$$

hence

$$\text{wt}_L^B(\mathbf{x} \star \mathbf{y}) \equiv \sum_{i,j} x_{ij} y_{ij} \pmod{2}.$$

Therefore,

$$\text{wt}_L^B(\mathbf{x} + \mathbf{y}) \equiv \text{wt}_L^B(\mathbf{x}) + \text{wt}_L^B(\mathbf{y}) - 2\text{wt}_L^B(\mathbf{x} \star \mathbf{y}) \pmod{4}.$$

If $\mathbf{x} \cdot \mathbf{y} = 0$ in $\mathbf{F}_{2^r}$, then

$$\sum_{i,j,k,\lambda} x_{ij} y_{ik} \gamma_\lambda^{(j,k)} b_\lambda = 0,$$

so, for every $1 \leq \lambda \leq r$,

$$\sum_{i,j,k} x_{ij} y_{ik} \gamma_\lambda^{(j,k)} = 0$$

in $\mathbf{F}_2$. Consequently,

$$\sum_{i,j} x_{ij} y_{ij} \equiv 0 \pmod{2},$$

so

$$\text{wt}_L^B(\mathbf{x} \star \mathbf{y}) \equiv 0 \pmod{2}. \quad \blacksquare$$

For the rest of this section, we assume $p^a = 2$ and m' odd. Recall also that, in this case, if C is a quasi-cyclic code over $\mathbf{F}_{2^r}$, then C_1 (over $\mathbf{F}_{2^r} + u\mathbf{F}_{2^r}$) is the component code of C corresponding to the factor $(Y - 1)^2$ of $Y^m - 1 = (Y^{m'} - 1)^2$.

LEMMA 7.2. *Let C be an ℓ -quasi-cyclic code over $\mathbf{F}_{2^r}$ of length ℓm . If the Lee weight of every codeword in C is divisible by 4, then the Lee weight of every codeword in C_1 is divisible by 4. Conversely, if every codeword in C_1 has Lee weight a multiple of 4, then all the codewords in C corresponding to $C_1 \times 0 \times \cdots \times 0$ also have Lee weights divisible by 4.*

Proof. For $\mathbf{x} + u\mathbf{y} \in C_1$, the image in C corresponding to $(\mathbf{x} + u\mathbf{y}, \mathbf{0}, \dots, \mathbf{0})$ is $(\mathbf{x} + \mathbf{y}, \mathbf{y}, \mathbf{x} + \mathbf{y}, \mathbf{y}, \dots, \mathbf{x} + \mathbf{y}, \mathbf{y})$. By definition,

$$\text{wt}_L^B(\mathbf{x} + u\mathbf{y}) = \text{wt}_L^B(\mathbf{x} + \mathbf{y}) + \text{wt}_L^B(\mathbf{y}),$$

where the Lee weight on the left-hand side refers to that of vectors over $\mathbf{F}_{2^r} + u\mathbf{F}_{2^r}$, while that on the right-hand side is that of vectors over $\mathbf{F}_{2^r}$. Hence,

$$\text{wt}_L^B(\mathbf{x} + \mathbf{y}, \mathbf{y}, \mathbf{x} + \mathbf{y}, \mathbf{y}, \dots, \mathbf{x} + \mathbf{y}, \mathbf{y}) = m' \text{wt}_L^B(\mathbf{x} + u\mathbf{y}).$$

As m' is odd, it follows that $\text{wt}_L^B(\mathbf{x} + u\mathbf{y})$ is divisible by 4 if and only if $\text{wt}_L^B(\mathbf{x} + \mathbf{y}, \mathbf{y}, \mathbf{x} + \mathbf{y}, \mathbf{y}, \dots, \mathbf{x} + \mathbf{y}, \mathbf{y})$ is divisible by 4. ■

LEMMA 7.3. *Let C be a self-orthogonal ℓ -quasi-cyclic code of length ℓm . For each $2 \leq \gamma \leq s$ (resp. $1 \leq \delta \leq t$), the codewords in C corresponding to $0 \times \dots \times 0 \times C_\gamma \times 0 \times \dots \times 0$ (resp. $0 \times \dots \times 0 \times C'_{s+\delta} \times 0 \times \dots \times 0$ and $0 \times \dots \times 0 \times C''_{s+\delta} \times 0 \times \dots \times 0$) all have Lee weights divisible by 4.*

Proof. We restrict our proof to the case of the codewords corresponding to $0 \times \dots \times 0 \times C_\gamma \times 0 \times \dots \times 0$. The case for $C'_{s+\delta}$ and $C''_{s+\delta}$ is identical except for notational differences.

In this case, using the same notation as in Theorem 6.2, the word $(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{m-1})$ in C corresponding to $(\mathbf{0}, \dots, \mathbf{0}, \mathbf{x} + u\mathbf{y}, \mathbf{0}, \dots, \mathbf{0}) \in 0 \times \dots \times 0 \times C_\gamma \times 0 \times \dots \times 0$ is given by (for $0 \leq j \leq m' - 1$),

$$\mathbf{c}_{2j} = \text{Tr}_\gamma(\mathbf{x}\zeta^{-2jz_\gamma}) + \text{Tr}_\gamma(\mathbf{y}\zeta^{(1-2j)z_\gamma}),$$

and

$$\mathbf{c}_{1+2j} = \text{Tr}_\gamma(\mathbf{y}\zeta^{-2jz_\gamma}),$$

where ζ is a primitive m' th root of 1.

Consider the minimal polynomial of $\omega_\gamma = \zeta^{-2z_\gamma}$ over $\mathbf{F}_2$. Since this is an irreducible polynomial of degree strictly greater than 1, it must have an odd number of terms. Let it be $1 + Y^{j_1} + \dots + Y^{j_{d-1}}$, where d is odd. Substituting $Y = \omega_\gamma$ and multiplying by ζ^{-2jz_γ} and $\zeta^{(1-2j)z_\gamma}$ respectively, we see that

$$\zeta^{-2(j+j_{d-1})z_\gamma} + \dots + \zeta^{-2(j+j_1)z_\gamma} + \zeta^{-2jz_\gamma} = 0$$

and

$$\zeta^{(1-2(j+j_{d-1}))z_\gamma} + \dots + \zeta^{(1-2(j+j_1))z_\gamma} + \zeta^{(1-2j)z_\gamma} = 0.$$

Consequently, it follows that

$$\mathbf{c}_{2(j+j_{d-1})} + \dots + \mathbf{c}_{2(j+j_1)} + \mathbf{c}_{2j} = \mathbf{0}$$

and

$$\mathbf{c}_{1+2(j+j_{d-1})} + \dots + \mathbf{c}_{1+2(j+j_1)} + \mathbf{c}_{1+2j} = \mathbf{0}.$$

Now let

$$\begin{aligned}
 \mathbf{u}_0^{(j)} &= \mathbf{c}_{2j}, \\
 \mathbf{u}_1^{(j)} &= \mathbf{c}_{2j} + \mathbf{c}_{2(j+j_1)}, \\
 \mathbf{u}_2^{(j)} &= \mathbf{c}_{2j} + \mathbf{c}_{2(j+j_1)} + \mathbf{c}_{2(j+j_2)}, \\
 &\vdots \\
 \mathbf{u}_{d-2}^{(j)} &= \mathbf{c}_{2j} + \mathbf{c}_{2(j+j_1)} + \cdots + \mathbf{c}_{2(j+j_{d-2})},
 \end{aligned}$$

and

$$\begin{aligned}
 \mathbf{v}_0^{(j)} &= \mathbf{c}_{1+2j}, \\
 \mathbf{v}_1^{(j)} &= \mathbf{c}_{1+2j} + \mathbf{c}_{1+2(j+j_1)}, \\
 \mathbf{v}_2^{(j)} &= \mathbf{c}_{1+2j} + \mathbf{c}_{1+2(j+j_1)} + \mathbf{c}_{1+2(j+j_2)}, \\
 &\vdots \\
 \mathbf{v}_{d-2}^{(j)} &= \mathbf{c}_{1+2j} + \mathbf{c}_{1+2(j+j_1)} + \cdots + \mathbf{c}_{1+2(j+j_{d-2})}.
 \end{aligned}$$

Then

$$\begin{aligned}
 \mathbf{c}_{2j} &= \mathbf{u}_0^{(j)}, \\
 \mathbf{c}_{2(j+j_1)} &= \mathbf{u}_0^{(j)} + \mathbf{u}_1^{(j)}, \\
 \mathbf{c}_{2(j+j_2)} &= \mathbf{u}_1^{(j)} + \mathbf{u}_2^{(j)}, \\
 &\vdots \\
 \mathbf{c}_{2(j+j_{d-2})} &= \mathbf{u}_{d-3}^{(j)} + \mathbf{u}_{d-2}^{(j)}, \\
 \mathbf{c}_{2(j+j_{d-1})} &= \mathbf{u}_{d-2}^{(j)},
 \end{aligned}$$

and

$$\begin{aligned}
 \mathbf{c}_{1+2j} &= \mathbf{v}_0^{(j)}, \\
 \mathbf{c}_{1+2(j+j_1)} &= \mathbf{v}_0^{(j)} + \mathbf{v}_1^{(j)}, \\
 \mathbf{c}_{1+2(j+j_2)} &= \mathbf{v}_1^{(j)} + \mathbf{v}_2^{(j)}, \\
 &\vdots \\
 \mathbf{c}_{1+2(j+j_{d-2})} &= \mathbf{v}_{d-3}^{(j)} + \mathbf{v}_{d-2}^{(j)}, \\
 \mathbf{c}_{1+2(j+j_{d-1})} &= \mathbf{v}_{d-2}^{(j)}.
 \end{aligned}$$

Therefore,

$$\begin{aligned}
 & d\text{wt}_L^B(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{m-1}) \\
 &= \sum_{j=0}^{m'-1} \text{wt}_L^B(\mathbf{c}_{2j}, \mathbf{c}_{2(j+j_1)}, \dots, \mathbf{c}_{2(j+j_{d-1})}, \mathbf{c}_{1+2j}, \mathbf{c}_{1+2(j+j_1)}, \dots, \mathbf{c}_{1+2(j+j_{d-1})}) \\
 &= \sum_{j=0}^{m'-1} \text{wt}_L^B(\mathbf{u}_0^{(j)}, \mathbf{u}_0^{(j)} + \mathbf{u}_1^{(j)}, \dots, \mathbf{u}_{d-3}^{(j)} + \mathbf{u}_{d-2}^{(j)}, \mathbf{u}_{d-2}^{(j)}, \mathbf{v}_0^{(j)}, \\
 &\quad \mathbf{v}_0^{(j)} + \mathbf{v}_1^{(j)}, \dots, \mathbf{v}_{d-3}^{(j)} + \mathbf{v}_{d-2}^{(j)}, \mathbf{v}_{d-2}^{(j)}) \\
 &\equiv 2w \pmod{4},
 \end{aligned}$$

where

$$w = \sum_{j=0}^{m'-1} \left(\sum_{i=0}^{d-2} \left(\text{wt}_L^B(\mathbf{u}_i^{(j)}) + \text{wt}_L^B(\mathbf{v}_i^{(j)}) \right) + \sum_{i=0}^{d-3} \left(\text{wt}_L^B(\mathbf{u}_i^{(j)} \star \mathbf{u}_{i+1}^{(j)}) + \text{wt}_L^B(\mathbf{v}_i^{(j)} \star \mathbf{v}_{i+1}^{(j)}) \right) \right).$$

Since C is ℓ -quasi-cyclic and self-orthogonal, applying $2k\ell$ times the cyclic shift to the word $(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{m-1})$ shows that

$$\sum_{j=0}^{m'-1} (\mathbf{c}_{2j} \cdot \mathbf{c}_{2(j+k)} + \mathbf{c}_{1+2j} \cdot \mathbf{c}_{1+2(j+k)}) \equiv 0 \pmod{2}.$$

It is easy to see that $\sum_{j=0}^{m'-1} (\text{wt}_L^B(\mathbf{u}_i^{(j)}) + \text{wt}_L^B(\mathbf{v}_i^{(j)}))$ is the linear combination of expressions of the type $\sum_{j=0}^{m'-1} (\mathbf{c}_{2j} \cdot \mathbf{c}_{2(j+k)} + \mathbf{c}_{1+2j} \cdot \mathbf{c}_{1+2(j+k)})$ for some set of k , so

$$\sum_{j=0}^{m'-1} (\text{wt}_L^B(\mathbf{u}_i^{(j)}) + \text{wt}_L^B(\mathbf{v}_i^{(j)})) \equiv 0 \pmod{2}.$$

Similarly, we deduce that

$$\sum_{j=0}^{m'-1} (\text{wt}_L^B(\mathbf{u}_i^{(j)} \star \mathbf{u}_{i+1}^{(j)}) + \text{wt}_L^B(\mathbf{v}_i^{(j)} \star \mathbf{v}_{i+1}^{(j)})) \equiv 0 \pmod{2}.$$

Therefore,

$$d\text{wt}_L^B(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{m-1}) \equiv 0 \pmod{4}.$$

Since d is odd, it follows that

$$\text{wt}_L^B(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{m-1}) \equiv 0 \pmod{4}.$$

■

THEOREM 7.4. *A self-dual ℓ -quasi-cyclic code C over $\mathbf{F}_{2^r}$ of length ℓm , where $m=2m'$ with m' odd, is of Type II if and only if its first component C_1 is of Type II over $\mathbf{F}_{2^r} + u\mathbf{F}_{2^r}$.*

Proof. Observe that C is the direct sum of its subcodes corresponding to $0 \times \cdots \times 0 \times C_\gamma \times 0 \times \cdots \times 0$, $0 \times \cdots \times 0 \times C'_{s+\delta} \times 0 \times \cdots \times 0$ and $0 \times \cdots \times 0 \times C''_{s+\delta} \times 0 \times \cdots \times 0$. Since C is self-dual, the theorem now follows from Lemmas 7.1–7.3, and Theorem 4.2.

Remark. Similar arguments also show that: a self-dual ℓ -quasi-cyclic code C over $\mathbf{F}_{2^r}$ of length ℓm , where m is odd, is of Type II if and only if its first component C_1 is of Type II over $\mathbf{F}_{2^r}$.

8. Generator Theory

A quasi-cyclic code C is 1-generator if and only if its generator matrix over the ring R contains only one row:

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

A study of 1-generator quasi-cyclic codes using the spectral approach, in the case where m is relatively prime to q , is found in [19]. Analogs of some of the results in [19] can be obtained for the complementary case where m is no longer relatively prime with q .

The *generator polynomial* of a 1-generator quasi-cyclic code is defined as

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

and its *parity-check polynomial* as $h(Y) := (Y^m - 1)/g(Y)$. (By convention, the GCD of polynomials is taken to be monic.)

For a code D of length ℓ over the chain ring $A = \mathbf{F}_{q^d} + u\mathbf{F}_{q^d} + \cdots + u^{p^a-1}\mathbf{F}_{q^d}$, we say that D is of depth δ if $D \subseteq u^\delta A^\ell$ and $D \not\subseteq u^{\delta+1}A^\ell$.

The following is a generalization of [19, Theorem 4.1].

THEOREM 8.1. *If C is a 1-generator ℓ -quasi-cyclic code, then it decomposes as*

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

where C_i (resp. C'_{s+j} and C''_{s+j}) is either trivial or a linear code over R_i (resp. R'_{s+j} and R''_{s+j}) generated by one nonzero codeword. The component codes C_i , C'_{s+j} and C''_{s+j} are of depth δ_i , δ'_{s+j} and δ''_{s+j} if and only if $g(Y) =$

$\in \prod_{i=1}^s f_i(Y)^{\delta_i} \prod_{j=1}^t f_{s+j}(Y)^{\delta'_{s+j}} f_{s+j}^*(Y)^{\delta''_{s+j}}$, where ϵ is a nonzero scalar. In this case, we have $\dim(C) = m - \deg(g)$. Conversely, every quasi-cyclic code C for which every C_i , C'_{s+j} and C''_{s+j} is generated by at most one codeword is a 1-generator quasi-cyclic code.

Proof. Suppose C is an ℓ -quasi-cyclic code with generator matrix

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

For each $1 \leq i \leq s$ (resp. $1 \leq j \leq t$), let $\xi_i \in F_i$ (resp. ξ'_{s+j} and ξ''_{s+j}) denote a root of f_i (resp. f_{s+j} and f_{s+j}^*), i.e., $f_i(\xi_i) = 0$ (resp. $f_{s+j}(\xi'_{s+j}) = 0$ and $f_{s+j}^*(\xi''_{s+j}) = 0$). Then it is clear that a generator matrix of C_i , C'_{s+j} and C''_{s+j} is given by

$$\begin{aligned} & (a_0(\xi_i(1-u)), a_1(\xi_i(1-u)), \dots, a_{\ell-1}(\xi_i(1-u))), \\ & (a_0(\xi'_{s+j}(1-u)), a_1(\xi'_{s+j}(1-u)), \dots, a_{\ell-1}(\xi'_{s+j}(1-u))), \\ & (a_0(\xi''_{s+j}(1-u)), a_1(\xi''_{s+j}(1-u)), \dots, a_{\ell-1}(\xi''_{s+j}(1-u))), \end{aligned}$$

respectively. Hence, C_i (resp. C'_{s+j} and C''_{s+j}) is either the trivial code or a linear code over R_i (resp. R'_{s+j} and R''_{s+j}) generated by one nonzero codeword.

For each $0 \leq \sigma \leq \ell - 1$, write $a_\sigma(Y) = \sum_{\tau=0}^{m-1} a_{\sigma\tau} Y^\tau$. Then,

$$a_\sigma(\xi_i(1-u)) = \sum_{k=0}^{p^a-1} (-1)^k u^k \xi_i^k \left(\sum_{\tau=k}^{m-1} a_{\sigma\tau} \xi_i^{\tau-k} \binom{\tau}{k} \right),$$

and similarly for expressions with ξ_i replaced by ξ'_{s+j} and ξ''_{s+j} .

It then follows readily that C_i (resp. C'_{s+j} and C''_{s+j}) is of depth δ_i (resp. δ'_{s+j} and δ''_{s+j}) if and only if, for all $0 \leq \sigma \leq \ell - 1$,

$$a_\sigma(\xi_i) = a_\sigma^{[1]}(\xi_i) = \dots = a_\sigma^{[\delta_i-1]}(\xi_i) = 0,$$

(resp.

$$a_\sigma(\xi'_{s+j}) = a_\sigma^{[1]}(\xi'_{s+j}) = \dots = a_\sigma^{[\delta'_{s+j}-1]}(\xi'_{s+j}) = 0$$

and

$$a_\sigma(\xi''_{s+j}) = a_\sigma^{[1]}(\xi''_{s+j}) = \dots = a_\sigma^{[\delta''_{s+j}-1]}(\xi''_{s+j}) = 0.)$$

By Proposition 2.1, it follows that C_i (resp. C'_{s+j} and C''_{s+j}) is of depth δ_i (resp. δ'_{s+j} and δ''_{s+j}) if and only if $f_i(Y)^{\delta_i}$ (resp. $f_{s+j}(Y)^{\delta'_{s+j}}$

and $f_{s+j}^*(Y)^{\delta''_{s+j}}$ divides $a_\sigma(Y)$ and $f_i(Y)^{\delta_i+1}$ (resp. $f_{s+j}(Y)^{\delta'_{s+j}+1}$ and $f_{s+j}^*(Y)^{\delta''_{s+j}+1}$) does not divide $a_\sigma(Y)$, for all $0 \leq \sigma \leq \ell - 1$. This is true if and only if $f_i(Y)^{\delta_i}$ (resp. $f_{s+j}(Y)^{\delta'_{s+j}}$ and $f_{s+j}^*(Y)^{\delta''_{s+j}}$) divides $g(Y)$ and $f_i(Y)^{\delta_i+1}$ (resp. $f_{s+j}(Y)^{\delta'_{s+j}+1}$ and $f_{s+j}^*(Y)^{\delta''_{s+j}+1}$) does not divide $g(Y)$.

Since $g(Y)$ is a monic factor of $Y^m - 1$, it follows therefore that C_i , C'_{s+j} and C''_{s+j} are of depth δ_i , δ'_{s+j} and δ''_{s+j} , for all $1 \leq i \leq s$ and $1 \leq j \leq t$ if and only if $g(Y) = \epsilon \prod_i f_i(Y)^{\delta_i} \prod_j f_{s+j}(Y)^{\delta'_{s+j}} f_{s+j}^*(Y)^{\delta''_{s+j}}$, where ϵ is a nonzero scalar.

Suppose that the fields F_i , F'_{s+j} and F''_{s+j} are extensions of $\mathbb{F}_q$ of degrees d_i , d'_{s+j} and d''_{s+j} , respectively. Note that $m' = \sum d_i + \sum d'_{s+j} + \sum d''_{s+j}$. The component code C_i (resp. C'_{s+j} and C''_{s+j}) is of depth δ_i (resp. δ'_{s+j} and δ''_{s+j}) implies that $|C_i| = q^{d_i(p^a - \delta_i)}$ (resp. $|C'_{s+j}| = q^{d'_{s+j}(p^a - \delta'_{s+j})}$ and $|C''_{s+j}| = q^{d''_{s+j}(p^a - \delta''_{s+j})}$). Hence, the size of C is given by

$$|C| = q^{p^a m' - (\sum d_i \delta_i + \sum d'_{s+j} \delta'_{s+j} + \sum d''_{s+j} \delta''_{s+j})}.$$

Since $g(Y) = \epsilon \prod_i f_i(Y)^{\delta_i} \prod_j f_{s+j}(Y)^{\delta'_{s+j}} f_{s+j}^*(Y)^{\delta''_{s+j}}$, so

$$\deg(g) = \sum d_i \delta_i + \sum d'_{s+j} \delta'_{s+j} + \sum d''_{s+j} \delta''_{s+j}.$$

Hence,

$$\dim(C) = m - \deg(g).$$

The final statement follows readily from the Chinese Remainder Theorem. ■

COROLLARY 8.2. *Let $\ell \geq 2$ and let C be a 1-generator ℓ -quasi-cyclic code with component codes C_i ($1 \leq i \leq s$) and C'_{s+j} , C''_{s+j} ($1 \leq j \leq t$) as in (2). Then the following statements are equivalent:*

- (i) $C^\perp$ is also a 1-generator ℓ -quasi-cyclic code;
- (ii) $\ell = 2$ and $|C_i| = |R_i|$, $|C'_{s+j}| = |R'_{s+j}| = |R''_{s+j}| = |C''_{s+j}|$, and C_i , C'_{s+j} and C''_{s+j} are all of depth 0, for all $1 \leq i \leq s$ and $1 \leq j \leq t$;
- (iii) $\ell = 2$ and $h(Y) = Y^m - 1$;
- (iv) $\ell = 2$ and $\dim(C) = m$.

Proof. Since C is a 1-generator quasi-cyclic code, it follows that $|C_i| \leq |R_i|$ ($1 \leq i \leq s$) and $|C'_{s+j}| \leq |R'_{s+j}|$, $|C''_{s+j}| \leq |R''_{s+j}|$ ($1 \leq j \leq t$).

The component codes of $C^\perp$ are $C_i^\perp$ ($1 \leq i \leq s$) and $(C'_{s+j})^\perp, (C''_{s+j})^\perp$ ($1 \leq j \leq t$). Statement (i) holds if and only if $|R_i|^\ell / |C_i| = |C_i^\perp| \leq |R_i|$ ($1 \leq i \leq s$) and $|R'_{s+j}|^\ell / |C'_{s+j}| = |(C'_{s+j})^\perp| \leq |R'_{s+j}|$, $|R''_{s+j}|^\ell / |C''_{s+j}| = |(C''_{s+j})^\perp| \leq |R''_{s+j}|$ ($1 \leq j \leq t$), which is equivalent to $\ell = 2$ and $|C_i| = |R_i|$, $|C'_{s+j}| = |R'_{s+j}| = |R''_{s+j}| = |C''_{s+j}|$ and C_i, C'_{s+j} and C''_{s+j} having depth 0, for all $1 \leq i \leq s$ and $1 \leq j \leq t$. The equivalence of (ii)–(iv) is obvious. ■

COROLLARY 8.3. *When $q = 2^r$ and $p^a = 2$, there are Type II 1-generator quasi-cyclic codes over $\mathbf{F}_q$ if and only if r is even.*

Proof. By Corollary 8.2, a Type II 1-generator quasi-cyclic code of the required sort must have $\ell = 2$. By Theorem 7.4, such a code exists if and only if there exists a Type II code of length 2 over $\mathbf{F}_{2^r} + u\mathbf{F}_{2^r}$. This latter code exists if and only if r is even [3, Theorem 15].

Similar results also hold for multigenerator codes. A quasi-cyclic code is said to be ρ -generator if ρ is the smallest integer such that C admits a generator matrix with ρ rows over $R(q, m)$.

Let k_i (resp. k'_{s+j} and k''_{s+j}) denote the minimum number of generators of C_i (resp. C'_{s+j} and C''_{s+j}) over R_i (resp. R'_{s+j} and R''_{s+j}). Denote by κ (resp. κ') the maximum (resp. minimum) of the k_i, k'_{s+j} and k''_{s+j} , for $i = 1, \dots, s$ and $j = 1, \dots, t$.

The proofs are similar to those for the 1-generator case, so we omit them.

THEOREM 8.4. *If C is a ρ -generator ℓ -quasi-cyclic code, then $\rho = \kappa$. More precisely, C decomposes under the CRT as*

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

with $\rho = \max\{k_i, k'_{s+j}, k''_{s+j}\}$, where C_i, C'_{s+j} and C''_{s+j} are linear codes over R_i, R'_{s+j} and R''_{s+j} with k_i, k'_{s+j} and k''_{s+j} generators, respectively.

Conversely, every quasi-cyclic code whose component codes C_i, C'_{s+j} and C''_{s+j} have k_i, k'_{s+j} and k''_{s+j} generators, respectively, is a ρ -generator quasi-cyclic code, where $\rho = \max\{k_i, k'_{s+j}, k''_{s+j}\}$. Furthermore, in this case, the dimension of C over $\mathbf{F}_q$ is $\leq \rho m$.

COROLLARY 8.5. *Let $\ell \geq 2$ and let C be a ρ -generator ℓ -quasi-cyclic code with component codes C_i ($1 \leq i \leq s$) and C'_{s+j}, C''_{s+j} ($1 \leq j \leq t$) as in (2). $l \geq 2\rho$ then the following statements are equivalent:*

- (i) $C^\perp$ is also a ρ -generator ℓ -quasi-cyclic code;
- (ii) $\ell = 2\rho$ and $|C_i| = |R_i|^\rho$, $|C'_{s+j}| = |R'_{s+j}|^\rho = |R''_{s+j}|^\rho = |C''_{s+j}|$, and C_i, C'_{s+j} and C''_{s+j} are all of depth 0, for all $1 \leq i \leq s$ and $1 \leq j \leq t$;
- (iii) $\ell = 2\rho$ and $\dim(C) = \rho m$.

9. Examples

In the following examples, we assume that q is a power of 2 and $p^a = 2$. The case where $q = 2$ is of special interest.

1. $m = 6$: Assume that $q = 2^t$ with t odd, so that we have the factorization into irreducible factors

$$Y^6 - 1 = (Y - 1)^2(Y^2 + Y + 1)^2,$$

so R decomposes into a product of $\mathbf{F}_q + u\mathbf{F}_q$ and $\mathbf{F}_{q^2} + u\mathbf{F}_{q^2}$, where $\mathbf{F}_q + u\mathbf{F}_q$ is equipped with the Euclidean inner product while $\mathbf{F}_{q^2} + u\mathbf{F}_{q^2}$ is equipped with the Hermitian inner product. Let ζ be a root of $Y^2 + Y + 1$ in $\mathbf{F}_{q^2}$. Then every ℓ -quasi-cyclic code C over $\mathbf{F}_q$ of length 6ℓ is given by

$$C = \{(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_5)\},$$

where, for $\mathbf{x}_0 + u\mathbf{x}_1 \in C_1$ and $(\mathbf{y}_0 + \zeta\mathbf{z}_0) + u(\mathbf{y}_1 + \zeta\mathbf{z}_1) \in C_2$ with C_1, C_2 the component codes of C over $\mathbf{F}_q + u\mathbf{F}_q$ and $\mathbf{F}_{q^2} + u\mathbf{F}_{q^2}$, respectively (note that $\mathbf{x}_0, \mathbf{x}_1, \mathbf{y}_0, \mathbf{y}_1, \mathbf{z}_0, \mathbf{z}_1$ are all in $\mathbf{F}_q^\ell$),

$$\begin{aligned} \mathbf{c}_0 &= \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{z}_0 + (\mathbf{y}_1 + \mathbf{z}_1), \\ \mathbf{c}_1 &= \mathbf{x}_1 + \mathbf{z}_1, \\ \mathbf{c}_2 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{y}_0 + \mathbf{z}_0) + \mathbf{y}_1, \\ \mathbf{c}_3 &= \mathbf{x}_1 + (\mathbf{y}_1 + \mathbf{z}_1), \\ \mathbf{c}_4 &= \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{y}_0 + \mathbf{z}_1, \\ \mathbf{c}_5 &= \mathbf{x}_1 + \mathbf{y}_1. \end{aligned}$$

2. Binary Golay code: Let $q = 2$ and continue to take $m = 6$. Let C_1 be the $\mathbf{F}_2 + u\mathbf{F}_2$ -code of length 4 with generator matrix

$$\begin{pmatrix} 1 & 0 & 1 & u \\ 0 & 1 & u & 1 \end{pmatrix}$$

and let C_2 be the $\mathbf{F}_4 + u\mathbf{F}_4$ -code $C'_2 + C'_2\zeta$, where $\zeta^2 + \zeta + 1 = 0$ and C'_2 is the $\mathbf{F}_2 + u\mathbf{F}_2$ -code of length 4 with generator matrix

$$\begin{pmatrix} 1 & 0 & u & 1+u \\ 0 & 1 & 1 & u \end{pmatrix}.$$

Then the 4-quasi-cyclic binary code C of length 24 obtained by the above construction (case $m=6$) is the binary Golay code. (This can be done through a computer check.)

It is easy to verify that C_1 and C_2 are self-dual, and that C_1 is in fact a Type II code over $\mathbf{F}_2 + u\mathbf{F}_2$, while it is well known that the binary Golay code is a Type II binary code. These facts verify Theorem 7.4. By Corollary 8.5, the binary Golay code is a 2-generator 4-quasi-cyclic code. It admits the following generator matrix over $R(2, 6)$ (as per Section 4):

$$\begin{pmatrix} 1 & 0 & 1+Y+Y^5 & 1+Y^2+Y^3+Y^4 \\ 0 & 1 & 1+Y+Y^3+Y^5 & 1+Y+Y^5 \end{pmatrix}.$$

3. $m=10$: We assume further that q is such that we have the factorization into irreducible factors

$$Y^{10} - 1 = (Y - 1)^2(Y^4 + Y^3 + Y^2 + Y + 1)^2,$$

so R decomposes into a product of $\mathbf{F}_q + u\mathbf{F}_q$ and $\mathbf{F}_{q^4} + u\mathbf{F}_{q^4}$, where $\mathbf{F}_q + u\mathbf{F}_q$ is equipped with the Euclidean inner product while $\mathbf{F}_{q^4} + u\mathbf{F}_{q^4}$ is equipped with the Hermitian inner product. Let ζ be a root of $Y^4 + Y^3 + Y^2 + Y + 1$ in $\mathbf{F}_{q^4}$. Then every ℓ -quasi-cyclic code C over $\mathbf{F}_q$ of length 10ℓ is given by

$$C = \{(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_9)\},$$

where, for $\mathbf{x}_0 + u\mathbf{x}_1 \in C_1$ and $(\mathbf{d}_0 + \zeta\mathbf{e}_0 + \zeta^2\mathbf{f}_0 + \zeta^3\mathbf{g}_0) + u(\mathbf{d}_1 + \zeta\mathbf{e}_1 + \zeta^2\mathbf{f}_1 + \zeta^3\mathbf{g}_1) \in C_2$ with C_1, C_2 the component codes of C over $\mathbf{F}_q + u\mathbf{F}_q$ and $\mathbf{F}_{q^4} + u\mathbf{F}_{q^4}$, respectively (note that $\mathbf{x}_i, \mathbf{d}_i, \mathbf{e}_i, \mathbf{f}_i, \mathbf{g}_i$ ($i=0, 1$) are all in $\mathbf{F}_q^\ell$),

$$\begin{aligned} \mathbf{c}_0 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{e}_0 + \mathbf{f}_0 + \mathbf{g}_0) + (\mathbf{d}_1 + \mathbf{e}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_1 &= \mathbf{x}_1 + (\mathbf{e}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_2 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{d}_0 + \mathbf{e}_0 + \mathbf{g}_0) + (\mathbf{d}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_3 &= \mathbf{x}_1 + (\mathbf{d}_1 + \mathbf{e}_1 + \mathbf{g}_1), \\ \mathbf{c}_4 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{d}_0 + \mathbf{e}_0 + \mathbf{f}_0 + \mathbf{g}_0) + (\mathbf{d}_1 + \mathbf{e}_1 + \mathbf{f}_1), \\ \mathbf{c}_5 &= \mathbf{x}_1 + (\mathbf{d}_1 + \mathbf{e}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_6 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{d}_0 + \mathbf{f}_0 + \mathbf{g}_0) + (\mathbf{e}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_7 &= \mathbf{x}_1 + (\mathbf{d}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_8 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{d}_0 + \mathbf{e}_0 + \mathbf{f}_0) + (\mathbf{d}_1 + \mathbf{e}_1 + \mathbf{g}_1), \\ \mathbf{c}_9 &= \mathbf{x}_1 + (\mathbf{d}_1 + \mathbf{e}_1 + \mathbf{f}_1). \end{aligned}$$

4. $m=14$: Assume that q is such that we have the factorization into irreducible factors

$$Y^{14} - 1 = (Y - 1)^2(Y^3 + Y + 1)^2(Y^3 + Y^2 + 1)^2,$$

so R decomposes into a product of $\mathbf{F}_q + u\mathbf{F}_q$ and two copies of $\mathbf{F}_{q^3} + u\mathbf{F}_{q^3}$, all equipped with the Euclidean inner product. Let ζ be a root of $Y^3 + Y + 1$ in $\mathbf{F}_{q^3}$. Then every ℓ -quasi-cyclic code C over $\mathbf{F}_q$ of length 14ℓ is given by

$$C = \{(\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{13})\},$$

where, for $\mathbf{x}_0 + u\mathbf{x}_1 \in C_1$, $(\mathbf{a}_0 + \zeta\mathbf{b}_0 + \zeta^2\mathbf{d}_0) + u(\mathbf{a}_1 + \zeta\mathbf{b}_1 + \zeta^2\mathbf{d}_1) \in C_2$ and $(\mathbf{e}_0 + \zeta^{-1}\mathbf{f}_0 + \zeta^{-2}\mathbf{g}_0) + u(\mathbf{e}_1 + \zeta^{-1}\mathbf{f}_1 + \zeta^{-2}\mathbf{g}_1) \in C_3$ with C_1, C_2, C_3 the component codes of C over $\mathbf{F}_q + u\mathbf{F}_q$ and $\mathbf{F}_{q^3} + u\mathbf{F}_{q^3}$, respectively (note that $\mathbf{x}_i, \mathbf{q}_i, \mathbf{b}_i, \mathbf{d}_i, \mathbf{e}_i, \mathbf{f}_i, \mathbf{g}_i$ ($i=0, 1$) are all in $\mathbf{F}_q^\ell$),

$$\begin{aligned} \mathbf{c}_0 &= \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{a}_0 + (\mathbf{e}_0 + \mathbf{f}_0 + \mathbf{g}_0) + \mathbf{d}_1 + (\mathbf{e}_1 + \mathbf{f}_1), \\ \mathbf{c}_1 &= \mathbf{x}_1 + \mathbf{a}_1 + (\mathbf{e}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_2 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{a}_0 + \mathbf{b}_0 + \mathbf{d}_0) + \mathbf{g}_0 + (\mathbf{a}_1 + \mathbf{b}_1) + (\mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_3 &= \mathbf{x}_1 + (\mathbf{a}_1 + \mathbf{b}_1 + \mathbf{d}_1) + \mathbf{g}_1, \\ \mathbf{c}_4 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{a}_0 + \mathbf{d}_0) + \mathbf{f}_0 + (\mathbf{b}_1 + \mathbf{d}_1) + \mathbf{e}_1, \\ \mathbf{c}_5 &= \mathbf{x}_1 + (\mathbf{a}_1 + \mathbf{d}_1) + \mathbf{f}_1, \\ \mathbf{c}_6 &= \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{d}_0 + (\mathbf{e}_0 + \mathbf{f}_0) + \mathbf{b}_1 + (\mathbf{e}_1 + \mathbf{g}_1), \\ \mathbf{c}_7 &= \mathbf{x}_1 + \mathbf{d}_1 + (\mathbf{e}_1 + \mathbf{f}_1), \\ \mathbf{c}_8 &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{a}_0 + \mathbf{b}_0) + (\mathbf{f}_0 + \mathbf{g}_0) + \mathbf{a}_1 + (\mathbf{e}_1 + \mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_9 &= \mathbf{x}_1 + (\mathbf{a}_1 + \mathbf{b}_1) + (\mathbf{f}_1 + \mathbf{g}_1), \\ \mathbf{c}_{10} &= \mathbf{x}_0 + \mathbf{x}_1 + (\mathbf{b}_0 + \mathbf{d}_0) + \mathbf{e}_0 + (\mathbf{a}_1 + \mathbf{b}_1 + \mathbf{d}_1) + \mathbf{g}_1, \\ \mathbf{c}_{11} &= \mathbf{x}_1 + (\mathbf{b}_1 + \mathbf{d}_1) + \mathbf{e}_1, \\ \mathbf{c}_{12} &= \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{b}_0 + (\mathbf{e}_0 + \mathbf{f}_0) + (\mathbf{a}_1 + \mathbf{d}_1) + \mathbf{f}_1, \\ \mathbf{c}_{13} &= \mathbf{x}_1 + \mathbf{b}_1 + (\mathbf{e}_1 + \mathbf{g}_1). \end{aligned}$$

10. Conclusion

In this article, an application of the GDFT and Hasse derivative has been given. Some new combinatorial constructions of quasi-cyclic codes have been introduced. It would be interesting, for decoding purposes, to explore the related trellises [23]. More examples need to be constructed to see if repeated-root quasi-cyclic codes are, or not, more promising than the quasi-cyclic codes with co-index coprime with the alphabet characteristic, cf. [5, 9–12]. The negative result for index one, i.e., the cyclic case, should not deter the interested researcher.

References

1. E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices, and invariant rings, *IEEE Transaction Information Theory*, Vol. 45 (1999) pp. 1194–1205.
2. K. Betsumiya, The Type II property for self-dual codes over finite fields of characteristic two, preprint.
3. K. Betsumiya, S. Ling and F. R. Nemenzo, Type II codes over $\mathbf{F}_{2^m} + u\mathbf{F}_{2^m}$, *Discrete Mathematics*, Vol. 275 (2004) pp. 43–65.
4. G. Castagnoli, J. L. Massey, P. A. Schoeller and N. von Seemann, On repeated-root cyclic codes, *IEEE Transactions on Information Theory*, Vol. 37 (1991) pp. 337–342.
5. Z. Chen, <http://www.tec.hkr.se/~chen/research/codes/>.
6. J. Conan and C. Séguin, Structural properties and enumeration of quasi-cyclic codes, *AAECC*, Vol. 4 (1993) pp. 25–39.
7. B. K. Dey, On existence of good self-dual quasi-cyclic codes, *IEEE Transactions on Information Theory*, Vol. 50 (2004) pp. 1794–1798.
8. S. T. Dougherty, P. Gaborit, M. Harada and P. Solé, Type II codes over $\mathbf{F}_2 + u\mathbf{F}_2$, *IEEE Transactions on Information Theory*, Vol. 45 (1999) pp. 32–45.
9. T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes, *IEEE Transactions on Information Theory*, Vol. 37 (1991) pp. 552–555.
10. T. A. Gulliver and V. K. Bhargava, Nine good $(m-1)/pm$ quasi-cyclic codes, *IEEE Transactions on Information Theory*, Vol. 38 (1992) pp. 1366–1369.
11. T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes over GF(3) and GF(4), *IEEE Transactions on Information Theory*, Vol. 38 (1992) pp. 1369–1374.
12. T. A. Gulliver and V. K. Bhargava, Twelve good rate $(m-r)/pm$ binary quasi-cyclic codes, *IEEE Transactions on Information Theory*, Vol. 39 (1993) pp. 1750–1751.
13. H. Hasse, Theorie der höheren Differentiale in einem algebraischen Funktionenkörper mit vollkommenem Konstantenkörper bei beliebiger Charakteristik, *J. Reine Angew. Math.*, Vol. 175 (1936) pp. 50–54.
14. K. Lally and P. Fitzpatrick, Algebraic structure of quasicyclic codes, *Disc. Appl. Math.*, Vol. 111 (2001) pp. 157–175.
15. R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, (1997).
16. S. Ling and P. Solé, Type II codes over $\mathbf{F}_4 + u\mathbf{F}_4$, *European J. Comb.*, Vol. 22 (2001) pp. 983–997.
17. S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE Transactions on Information Theory*, Vol. 47 (2001) pp. 2751–2760.
18. S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes II: chain rings, *Des., Codes and Crypto.*, Vol. 30 (2003) pp. 113–130.
19. S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes III: generator theory, *IEEE Transactions on Information Theory*, Vol. 51 (2005) 2692–2700.
20. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland, Amsterdam (1977).
21. J. L. Massey and S. Sercone, *Linear complexity of periodic sequences: a general theory*, Advances in Cryptology—Crypto '96 (N. Koblitz ed.), LNCS 1109 (1996), pp. 358–371.
22. B. R. McDonald, *Finite Rings with Identity*, Marcel Dekker, New York (1974).
23. A. Vardy, *Trellis structure of codes*, in *Handbook of Coding Theory*, Vol. II, V. S. Pless and W. C. Huffman (eds.), Elsevier Science, Amsterdam (1998) pp. 1989–2117.