On the algebraic structure of quasi-cyclic codes II : chain rings

Ling, San; Sole, Patrick

2003

Ling, S., & Solé, P. (2003). On the Algebraic Structure of Quasi-cyclic Codes II: Chain Rings Designs. Codes and Cryptography, 30(1), 113-130.

https://hdl.handle.net/10356/96415

https://doi.org/10.1023/A:1024715527805

On the Algebraic Structure of Quasi-cyclic Codes II: Chain Rings

SAN LING* lings@math.nus.edu.sg
Department of Mathematics, National University of Singapore, Singapore 117543

PATRICK SOLÉ ps@essi.fr
CNRS, I3S, ESSI, BP 145, Route des Colles, 06 903 Sophia Antipolis, France

Communicated by: G. Mullen

Abstract. The ring decomposition technique of part I is extended to the case when the factors in the direct product decomposition are no longer fields but arbitrary chain rings. This includes not only the case of quasi-cyclic codes over rings but also the case of quasi-cyclic codes over fields whose co-index is no longer prime to the characteristic of the field. A new quaternary construction of the Leech lattice is derived.

AMS Classification: 94B05, 94B15, 11T71

1. Introduction

In this work, following the approach of part I [21] we propose to view quasi-cyclic codes over a finite commutative ring A as codes over the polynomial ring $R(A,m) := A[Y]/(Y^m - 1)$. This latter ring can be decomposed into a direct sum of local rings. (When $R(A,m)$ is principal we obtain as direct summands chain rings—a class of rings of current interest in coding theory [24,25]). This can be achieved by either the Chinese Remainder Theorem or the Discrete Fourier Transform. We emphasize the fact that codes over chain rings can shed new light on codes over fields. This occurs when $A = \mathbf{F}_q$ and $(m,q) > 1$.

The benefits of this novel approach are twofold. Firstly, we can investigate self-dual quasi-cyclic codes in a systematic way. Secondly, we can decompose quasi-cyclic codes into codes of lower lengths. The composition products that occur are very well-known [30] in the area of trellis decoding: twisted squaring [2], cubing [9], ternary cubing [18], $(\mathbf{u}+\mathbf{v}\,|\,\mathbf{u}-\mathbf{v})$ [16] and Vandermonde [15]. In the same vein, we derive a new $\mathbf{Z}_4$ construction of the Leech lattice along the lines of Forney's construction [9]. New constructions (quinting, septing) are introduced as well.

*Corresponding author.

We hope that a future impact of this work will be more efficient trellises for more block codes and more lattices.

The paper is organized in the following way. Section 2 contains some basic notations and definitions. Section 3 discusses the correspondence between quasi-cyclic codes over a ring A with linear codes over $R(A,m)$. Section 4 develops the alphabet decomposition using the Chinese Remainder Theorem. Section 5 tackles the same problem with the Discrete Fourier Transform which results in a trace representation for quasi-cyclic codes that generalizes nicely the trace representation of cyclic codes and linearly recurring sequences. Section 6 develops applications of the above theory, firstly for small lengths of the composition codes (e.g., double circulant codes), secondly for large lengths. In Section 7, we include a discussion on Type II quasi-cyclic codes. An appendix collects the necessary material on permutation groups of codes. In particular, we give as examples affine-invariant and extended quadratic residue codes.

2. Notations and Definitions

2.1. *Rings*

A commutative ring A is local if it admits a unique maximal ideal M. In that case the quotient ring $k := A/M$ is a field. Factorizations fg of elements h of $k[X]$ can be "lifted" to factorizations FG of H in A in such a way that f, g, h correspond to F, G, H respectively under reduction modulo M. This is the so-called Hensel lifting. For the special case of $A = \mathbf{Z}_4$, so $k = \mathbf{F}_2$, see for instance Bonnecaze et al. [3].

A ring is a chain ring if and only if it is both local and principal. A local ring is a chain ring if and only if its maximal ideal has a unique generator t, say: $M = (t)$. With these notations the ideals of A constitute a chain for inclusion

$$A \supset (t) \supset (t^2) \supset \cdots \supset (t^{d-1}) \supset (t^d) = (0).$$

The integer d is then called the depth of A. If k, as a finite field, has q elements, then $A/(t^i)$ has q^i elements, so A has q^d elements.

2.2. *Codes*

A linear code of length n over a finite commutative ring A (with identity) is an A-submodule of A^n. We denote by T the standard shift operator on A^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. Throughout the paper we shall assume that the index ℓ divides the length n, and we will call $m := n/\ell$ the co-index. 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 [22]. More generally, up to equivalence, the generator matrix of such a code consists of $m \times m$ circulant matrices. This point will be elaborated upon in Lemma 3.1 below.

3. Quasi-Cyclic Codes

Let A be a finite chain ring and let m be a positive integer. Let $R := R(A, m) = A[Y]/(Y^m - 1)$.

Let C be a quasi-cyclic code over A 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 $\phi : A^{\ell m} \to R^{\ell}$ 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.

LEMMA 3.1. *The map ϕ induces a one-to-one correspondence between quasi-cyclic codes over A of index ℓ and length ℓm and linear codes over R of length ℓ.*

The proof of Lemma 3.1 is similar to that of [21, Lemma 3.1], so we omit it here.

We define a "conjugation" map on R as one that acts as the identity on the elements of A and that sends Y to $Y^{-1} = Y^{m-1}$, and extended linearly.

We define on $A^{\ell m}$ 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 $\mathbf{y} = (y_0, \dots, y_{\ell-1})$,

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

We omit the proof of the following proposition. It is analogous to that of [21, Proposition 3.2].

PROPOSITION 3.2. *Let* $\mathbf{a}, \mathbf{b} \in A^{\ell m}$*. Then* $\left(T^{\ell k}(\mathbf{a})\right) \cdot \mathbf{b} = 0$ *for all* $0 \leq k \leq m-1$ *if and only if* $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$.

By applying Proposition 3.2 with $\mathbf{a}$ belonging to an ℓ-quasi-cyclic code C of length ℓm over A, we obtain.

COROLLARY 3.3. *Let* C *be a quasi-cyclic code over* A *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* $A^{\ell m}$ *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* A *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 $R(A, m)$

When $m > 1$, the ring $R(A, m) = A[Y]/(Y^m - 1)$ is never a local ring. However, a finite commutative ring always decomposes into a product of local rings. We study this decomposition in our present context to facilitate our study of quasi-cyclic codes over finite chain rings.

Let the characteristic of the finite chain ring A be p^n, where p is a prime. Write $m = p^a m'$, where $(m', p) = 1$. The polynomial $Y^{m'} - 1$ factors completely into distinct irreducible factors in $k[Y]$, so by Hensel's lifting, we may write $Y^{m'} - 1 \in A[Y]$ as

$$Y^{m'} - 1 = f_1 f_2 \ldots f_r,$$

where f_j are distinct basic irreducible polynomials. This product is unique in the sense that, if $Y^{m'} - 1 = f_1' f_2' \ldots f_s'$ is another decomposition into basic irreducible polynomials, then $r = s$ and, after suitable renumbering of the f_j''s, we have that f_j is an associate of f_j', for each $1 \leq j \leq r$.

For a polynomial f, let f^* denote its reciprocal polynomial. Note that $(f^*)^* = f$. We have therefore

$$Y^{m'} - 1 = -f_1^* f_2^* \cdots f_r^*.$$

If f is a basic irreducible polynomial, so is f^*. By the uniqueness of such a decomposition into basic irreducible factors, we can now write

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

where δ is a unit in A, $g_1, \ldots, g_s$ are those f_j's that are associates to their own reciprocals, and $h_1, h_1^*,$ to h_t, h_t^* are the remaining f_j's grouped in pairs.

Now we suppose further that, if the characteristic of A is p^n, where $n > 1$, then $a = 0$, i.e., $m = m'$ is relatively prime to p. When the characteristic of A is p (such as in the case where A is a finite field), m need not be relatively prime to p. Then it follows that, in $A[Y]$, we have

$$Y^m - 1 = Y^{p^a m'} - 1 = (Y^{m'} - 1)^{p^a} = \delta^{p^a} g_1^{p^a} \cdots g_s^{p^a} h_1^{p^a} (h_1^*)^{p^a} \cdots h_t^{p^a} (h_t^*)^{p^a}.$$

Consequently, we may now write

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

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 $A[Y]/(g_i)^{p^a}$ by G_i, $A[Y]/(h_j)^{p^a}$ by H_j' and $A[Y]/(h_j^*)^{p^a}$ by H_j''.

It follows from (1) that

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

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

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

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.

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

$$(c_1(Y), \ldots, c_s(Y), c_1'(Y), c_1''(Y), \ldots, c_t'(Y), c_t''(Y)), \tag{2}$$

where $c_i(Y) \in G_i (1 \le i \le s), c_j'(Y) \in H_j'$ and $c_j''(Y) \in H_j'' (1 \le j \le t)$. Of course, the c_i, c_j' and c_j'' may also be considered as polynomials in $A[Y]$.

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

$$\mathbf{r} = (r_1, \ldots, r_s, r_1', r_1'', \ldots, r_t', r_t''),$$

where $r_i \in G_i$ $(1 \le i \le s)$, $r_j' \in H_j'$ and $r_j'' \in H_j''$ $(1 \le j \le t)$. We shall now describe $\bar{\mathbf{r}}$ in terms of the decomposition (1).

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

$$\frac{A[Y]}{(f)} \longrightarrow \frac{A[Y]}{(f^*)}$$

$$c(Y) + (f) \mapsto c(Y^{-1}) + (f^*). \tag{3}$$

(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 (3) that the map $Y \mapsto Y^{-1}$ induces an automorphism of $A[Y]/(f)$. For $r \in A[Y]/(f)$, we denote by $\overline{r}$ its image under this induced map. When the degree of f is 1, note that the induced map is the identity map, so $\overline{r} = r$.

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

$$(\overline{r_1}, \ldots, \overline{r_s}, r_1'', r_1', \ldots, r_t'', r_t').$$

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

$$\langle \mathbf{c}, \mathbf{c}' \rangle = \sum_{i=1}^{\ell} c_i \overline{c_i'}. \tag{4}$$

Remark. In the case where the degree of f is 1, since the map $r \mapsto \overline{r}$ is the identity, the Hermitian inner product (4) is none other than the usual Euclidean inner product on A (cf. Section 3).

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*

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

and

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

Decomposing each $\mathbf{a}_i, \mathbf{b}_i$ *using* (2), *we write*

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

and

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

where $a_{ij}, b_{ij} \in G_j$, $a'_{ij}, b'_{ij}, a''_{ij}, b''_{ij} \in H'_j$ *(with* H'_j *and* H''_j *identified). Then*

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

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

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

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

5. Fourier Transform

In the case where m and the characteristic of A are relatively prime, hence m is a unit in A, the isomorphism (1) can in fact be described in a more explicit way via the discrete Fourier Transform.

Suppose that A is a finite chain ring with maximal ideal (t) such that the residue field $k = A/(t)$ is $\mathbf{F}_q$. Every element x of A can be expressed uniquely in the form

$$x = x_0 + x_1 t + \cdots + x_{d-1} t^{d-1},$$

where $x_0, \ldots, x_{d-1}$ belong to the Teichmüller set. Since g_i, h_j, h^*_j are monic basic irreducible polynomials, the rings G_i, H'_j and H''_j are Galois extensions of A. Since Galois extensions of a local ring are unramified, the unique maximal ideal in such a Galois extension of A is again generated by t. For a Galois extension B of A, we define the Frobenius map F on B to be the map induced by the map $Y \mapsto Y^q$, acting as the identity on A. If the degree of the extension B over A is e, then F^e is the identity map. For $x \in B$, we define the trace of x to be

$$Tr_{B/A}(x) = x + F(x) + \cdots + F^{e-1}(x).$$

In (1), the direct factors on the right hand side correspond to the irreducible factors of $Y^m - 1$ in $A[Y]$. There is a one-to-one correspondence between these factors and the q-cyclotomic cosets of $\mathbf{Z}/m\mathbf{Z}$, where q is the order of the residue field $A/(t)$. Denote by $U_i (1 \le i \le s)$ the cyclotomic coset corresponding to g_i, V_j and W_j $(1 \le j \le t)$ the cyclotomic cosets corresponding to h_j and h_j^*, respectively.

For $\mathbf{c} = \sum_{g \in \mathbf{Z}/m\mathbf{Z}} c_g Y^g \in A[Y]/(Y^m - 1)$, its Fourier Transform is $\hat{\mathbf{c}} = \sum_{h \in \mathbf{Z}/m\mathbf{Z}} \hat{c}_h Y^h$, where the Fourier coefficient $\hat{c}_h$ is defined as

$$\hat{c}_h = \sum_{g \in \mathbf{Z}/m\mathbf{Z}} c_g \zeta^{gh},$$

where ζ is a primitive m-th root of 1 in some (sufficiently large) Galois extension of A. The inverse transform is given by

$$c_g = m^{-1} \sum_{h \in \mathbf{Z}/m\mathbf{Z}} \hat{c}_h \zeta^{-gh}.$$

It is well-known that $\hat{c}_{qh} = F(\hat{c}_h)$ and, for $h \in U_i$, $\hat{c}_h \in G_i$, while for $h \in V_j$ (resp. W_j), $\hat{c}_h \in H_j'$ (resp. H_j''). In fact, the Fourier Transform gives rise to the isomorphism (1). The inverse is given by the inverse transform, which can be expressed as follows. Let G_i, H_j' and H_j'' denote the Galois extensions of A corresponding to the polynomials g_i, h_j and h_j^*, with corresponding cyclotomic cosets U_i, V_j and W_j. For each i, choose and fix some $u_i \in U_i$. For each j, choose and fix some $v_j \in V_j$ and $w_j \in W_j$. Let $\hat{c}_i \in G_i$, $\hat{c}_j' \in H_j'$ and $\hat{c}_j'' \in H_j''$. To the $(s + 2t)$-tuple $(\hat{c}_1, \ldots, \hat{c}_s, \hat{c}_1', \hat{c}_1'', \ldots, \hat{c}_t', \hat{c}_t'')$, we associate the element $\sum_{g \in \mathbf{Z}/m\mathbf{Z}} c_g Y^g \in A[Y]/(Y^m - 1)$, where

$$mc_g = \sum_{i=1}^{s} Tr_{G_i/A}(\hat{c}_i \zeta^{-gu_i}) + \sum_{j=1}^{t} (Tr_{H_j'/A}(\hat{c}_j' \zeta^{-gv_j}) + Tr_{H_j''/A}(\hat{c}_j'' \zeta^{-gw_j})),$$

where $Tr_{B/A}$ denotes the trace from B to A. For a vector $\mathbf{x}$, by its Fourier Transform, we simply mean the vector whose i-th entry is the Fourier Transform of the i-th entry of $\mathbf{x}$. By the trace of $\mathbf{x}$, we mean the vector whose coordinates are the traces of the coordinates of $\mathbf{x}$.

This description gives the following characterization result on quasi-cyclic codes over finite chain rings A, where m is relatively prime to the characteristic of A.

THEOREM 5.1. *Let m be an integer relatively prime to the characteristic of A. Then, for any ℓ, the quasi-cyclic codes over A of length ℓm and of index ℓ are precisely given by the following construction: write $Y^m - 1 = \delta g_1 \ldots g_s h_1 h_1^* \ldots h_t h_t^*$, where δ is a unit of A, g_i are irreducible factors that are associates to their own reciprocals, and h_j are irreducible factors whose reciprocals are h_j^*. Write $A[Y]/(g_i) = G_i$, $A[Y]/(h_j) = H_j'$ and $A[Y]/(h_j^*) = H_j''$. Let U_i (resp. V_j and W_j) denote the q-cyclotomic coset of $\mathbf{Z}/m\mathbf{Z}$*

corresponding to G_i (resp. H'_j and H''_j) and fix $u_i \in U_i$, $v_j \in V_j$ and $w_j \in W_j$. For each i, let C_i be a code of length ℓ over G_i, and for each j, let C'_j be a code of length ℓ over H'_j and let C''_j be a code of length ℓ over H''_j. For $\mathbf{x}_i \in C_i$, $\mathbf{y}'_j \in C'_j$ and $\mathbf{y}''_j \in C''_j$, and for each $0 \le g \le m-1$, let

$$\mathbf{c}_g = \sum_{i=1}^{s} Tr_{G_i/A}(\mathbf{x}_i \zeta^{-gu_i}) + \sum_{j=1}^{t} (Tr_{H'_j/A}(\mathbf{y}'_j \zeta^{-gv_j}) + Tr_{H''_j/A}(\mathbf{y}''_j \zeta^{-gw_j})).$$

Then the code

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

is a quasi-cyclic code over A of length ℓm and of index ℓ. Conversely, every quasi-cyclic code over A 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 $C''_j = (C'_j)^{\perp}$ for each j with respect to the Euclidean inner product.

Remark. In the definition of $\mathbf{c}_g$ in Theorem 5.1, the m has been suppressed. Note that m is a unit in A, so $mC = C$.

6. Applications

We now apply our earlier discussions to several situations. We can either start with a (small) fixed ℓ or a (small) fixed m. We give examples of both cases.

6.1. Quasi-cyclic Codes of Index 2

Let $\ell = 2$ and let $\mathbf{F}_q$ be any finite field. Suppose first that m is relatively prime to q. The decomposition (1) shows that R is the direct sum of finite extensions of $\mathbf{F}_q$.

Self-dual codes (with respect to the Euclidean inner product) of length 2 over a finite field $\mathbf{F}_q$ exist if and only -1 is a square in $\mathbf{F}_q$, which is the case when one of the following is true:

1. q is a power of 2;
2. $q = p^b$, where p is a prime congruent to 1 mod 4; or
3. $q = p^{2b}$, where p is a prime congruent to 3 mod 4.

In this case, up to equivalence, there is a unique self-dual code of length 2 over $\mathbf{F}_q$, viz. the one with generator matrix $(1, i)$, where i denotes a square root of -1 in $\mathbf{F}_q$.

This enables one to characterize the self-dual quasi-cyclic codes over $\mathbf{F}_q$ of length $2m$ and of index 2, where m is relatively prime to q, once the irreducible factors of $Y^m - 1$ are known. This characterization is summarized in [21, Proposition 6.1]. In fact, using facts on finite chain rings, the restriction that m be relatively prime to q can be removed.

THEOREM 6.1. *Let m be any positive integer. Then self-dual 2-quasi-cyclic codes over* $\mathbf{F}_q$ *of length 2m exist if and only if exactly one of the following conditions is satisfied*:

1. *q is a power of 2*;

2. $q = p^b$*, where p is a prime congruent to 1 mod 4; or*

3. $q = p^{2b}$*, where p is a prime congruent to 3 mod 4.*

Proof. By [21, Proposition 6.1], we may now assume that $q = p^b$ and $m = p^a m'$, where $a > 0$. It follows from (1) that the G_i are finite chain rings of depth p^a. A self-dual 2-quasi-cyclic code over $\mathbf{F}_q$ of length $2m$ exists if and only if, for each i, there exists a self-dual linear code of length 2 over G_i.

From now on, for simplicity of notation, we suppress the suffix i in G_i. Let G denote a finite chain ring of depth $d = p^a$, with maximal ideal (t) and residue field $\mathbf{F}_{q^e}$. Therefore, G has q^{de} elements.

We first prove the sufficiency of the conditions in the Theorem. If any of the conditions in the statement of the Theorem is satisfied, then $X^2 + 1 = 0$ has a solution in the residue field $G/(t) = \mathbf{F}_{q^e}$, and such a solution lifts to a solution in $G/(t^c)$, for any $1 \le c \le d$ (cf. [23, pp. 270–271]). In particular, there exists an $i \in G$ such that $i^2 + 1 = 0$. It is clear that the free code with generator matrix $(1, i)$ is self-dual of length 2.

Next we prove the necessity. It suffices to consider the case where q is odd, since the case where q is even is trivially true.

In this case, we look at the component G_1 corresponding to the polynomial $Y - 1$ in (1) and let $G = G_1$. The depth d is odd. In fact, $G = \mathbf{F}_q[t]/(t)^{p^a}$ and the map $Y \mapsto Y^{-1}$ induces the identity map on G. (Therefore, the Hermitian inner product and the Euclidean inner product coincide in this case.) Any nonzero element of G can be expressed as $t^\lambda u$, where u is a unit in G. A nonzero codeword of length 2 is therefore of one of the forms: (i) $(0, t^\mu v)$, (ii) $(t^\lambda u, 0)$ or (iii) $(t^\lambda u, t^\mu v)$.

For a word of form (i) to be self-orthogonal, we must have $\mu \ge d + 1/2$. For a word of type (ii) to be self-orthogonal, we need $\lambda \ge d + 1/2$. For a word of type (iii) to be self-orthogonal, we need

$$t^{2\lambda}u^2 + t^{2\mu}v^2 = 0. \tag{5}$$

If both $\lambda, \mu \ge d + 1/2$, then (5) is automatically satisfied. Next suppose at least one of them is at most $d - 1/2$. In this case, if $\lambda \ne \mu$, then it is easy to see that (5) is never satisfied. Hence, in order for (5) to be satisfied, we need $\lambda = \mu$. Then (5) implies

$$u^2 + v^2 \in (t^{d-2\lambda}). \tag{6}$$

This means, in particular, that $u^2 + v^2 \in (t)$, so -1 is a square in $\mathbf{F}_q$. A self-dual code of length 2 over G certainly contains at least a codeword of type (iii), for there are not enough words of the other types to form such a code. Therefore, the conditions in the statement of the Theorem are certainly necessary.

The Theorem is now proved. ■

When m is divisible by p, where p is a prime such that $q = p^b$, writing $m = p^a m'$ as before, the factors on the right hand side of (1) are no longer finite fields. They are, however, finite chain rings of depth p^a. Therefore, to classify the self-dual quasi-cyclic codes over $\mathbf{F}_q$ of index 2 and of length $2m$, we will first need a classification of self-dual codes of length 2 over finite chain rings of depth p^a.

6.2. *m* = 3 *and the Leech Lattice*

Assume $m = 3$ and let $A = \mathbf{Z}_4$. We denote by $GR(4,2)$ the unique Galois extension of $\mathbf{Z}_4$ of degree 2. The ring R now decomposes into the direct sum $\mathbf{Z}_4 \oplus GR(4,2)$. An ℓ-quasi-cyclic code C over $\mathbf{Z}_4$ of length 3ℓ now decomposes into a pair (C_1, C_2), where C_1 is a code over $\mathbf{Z}_4$ of length ℓ and C_2 is a code of length ℓ over $GR(4,2)$. This correspondence is given by

$$C = \{(\mathbf{x} + 2\mathbf{a}' - \mathbf{b}' \,|\, \mathbf{x} - \mathbf{a}' + 2\mathbf{b}' \,|\, \mathbf{x} - \mathbf{a}' - \mathbf{b}') \,|\, \mathbf{x} \in C_1, \mathbf{a}' + \zeta\mathbf{b}' \in C_2\},$$

where $\zeta \in GR(4,2)$ satisfies $\zeta^2 + \zeta + 1 = 0$.

If we take a linear code C_2' of length ℓ over $\mathbf{Z}_4$, we see that $C_2 := C_2' + C_2'\zeta$ is a linear code over $GR(4,2)$. If C_2 is obtained by such an extension of scalar from a $\mathbf{Z}_4$-code C_2', by a change of variable $\mathbf{a} = -2\mathbf{a}' + \mathbf{b}'$ and $\mathbf{b} = -\mathbf{a}' + 2\mathbf{b}'$, we see immediately that this construction is equivalent to the $(\mathbf{x} - \mathbf{a} \,|\, \mathbf{x} + \mathbf{b} \,|\, \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction, with $\mathbf{x} \in C_1$ and $\mathbf{a}, \mathbf{b} \in C_2'$.

Now let C_2' be the Klemm-like code κ_8 (over $\mathbf{Z}_4$) [3] and let C_1 be the self-dual $\mathbf{Z}_4$-code O_8', obtained from the octacode O_8 by negating a single coordinate. Let (cf. [3])

$$\kappa_8 \Delta O_8' := \{(\mathbf{x} - \mathbf{a} \,|\, \mathbf{x} + \mathbf{b} \,|\, \mathbf{x} + \mathbf{a} - \mathbf{b}) \,|\, \mathbf{x} \in O_8', \mathbf{a}, \mathbf{b} \in \kappa_8\}.$$

For a $\mathbf{Z}_4$-linear code C of length n, let the quaternary lattice $\Lambda(C)$ be defined as

$$\Lambda(C) = \{\mathbf{z} \in \mathbf{Z}^n \,|\, \mathbf{z} \equiv \mathbf{c} \bmod 4 \text{ for some } \mathbf{c} \in C\}.$$

THEOREM 6.2. $\Lambda(\kappa_8 \Delta O_8')/2$ *is the Leech lattice* Λ_{24}.

Proof. From the way we obtained the $(\mathbf{x} - \mathbf{a} \,|\, \mathbf{x} + \mathbf{b} \,|\, \mathbf{x} + \mathbf{a} - \mathbf{b})$ construction above, it is clear that $\kappa_8 \Delta O_8'$ is self-dual.

The code is generated by vectors $(-\mathbf{a}, \mathbf{0}, \mathbf{a})$, $(\mathbf{0}, \mathbf{b}, -\mathbf{b})$ and $(\mathbf{x}, \mathbf{x}, \mathbf{x})$, where $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in O'_8$. All these vectors have Euclidean weights congruent to 0 mod 8. Hence all the words in the code have weights divisible by 8. By [3, Theorem 4.1], $\Lambda(\kappa_8 \Delta O'_8)$ is an even unimodular lattice.

From the proof of [3, Theorem 4.5], we have that $\kappa_8 \cap O'_8 = 2O'_8$. It remains to show that the minimum Euclidean weight in the lattice is at least 16.

Suppose that the Euclidean weight of $(\mathbf{x} - \mathbf{a} \,|\, \mathbf{x} + \mathbf{b} \,|\, \mathbf{x} + \mathbf{a} - \mathbf{b})$, for some $\mathbf{a}, \mathbf{b} \in \kappa_8$ and $\mathbf{x} \in O'_8$, is equal to 8. Mimicking the proof of [3, Theorem 4.5], we see that $\mathbf{x} \equiv \mathbf{0} \mod 2$ and also $\mathbf{a} \equiv \mathbf{b} \equiv \mathbf{0} \mod 2$. Then $(\mathbf{x} - \mathbf{a} \,|\, \mathbf{x} + \mathbf{b} \,|\, \mathbf{x} + \mathbf{a} - \mathbf{b}) = (\mathbf{x} + \mathbf{a} \,|\, \mathbf{x} + \mathbf{b} \,|\, \mathbf{x} + \mathbf{a} + \mathbf{b})$, and the argument in loc. cit. shows that such a word has Euclidean weight at least 16. ■

6.3. $m = 6$ and the Golay Code

Next we let $m = 6$ and assume $A = \mathbf{F}_2$. Then

$$R = (\mathbf{F}_2 + u\mathbf{F}_2) \oplus (\mathbf{F}_4 + u\mathbf{F}_4),$$

where $\mathbf{F}_2 + u\mathbf{F}_2 = \mathbf{F}_2[Y]/(Y-1)^2$ and $\mathbf{F}_4 + u\mathbf{F}_4 = \mathbf{F}_2[Y]/(Y^2 + Y + 1)^2$, so $u^2 = 0$ in both $\mathbf{F}_2 + u\mathbf{F}_2$ and $\mathbf{F}_4 + u\mathbf{F}_4$.

Let C_1 be the unique $\mathbf{F}_2 + u\mathbf{F}_2$-code of length 4 whose Gray image is the binary extended Hamming code with the coordinates in reverse order (cf. [6]) and let C_2 be the $\mathbf{F}_4 + u\mathbf{F}_4$-code $C'_2 + C'_2\zeta$, where C'_2 is the unique $\mathbf{F}_2 + u\mathbf{F}_2$-code of length 4 whose Gray image is the binary extended Hamming code. Since both C_1 and C_2 are self-dual, we see that this is yet another way to regard the binary Golay code.

PROPOSITION 6.3. *The binary extended Golay code is 4-quasi-cyclic.*

Remark. Clearly the 8-quasi-cyclicity (see [21, Corollary 6.8]) follows from Proposition 6.3. In fact, from Corollary A.3 of the Appendix, and the fact that the binary extended Golay code is in fact an extended quadratic residue code of length $p + 1$, where $p = 23$, we have that the binary extended Golay code is in fact 2-quasi-cyclic. Proposition 6.3 is therefore a corollary of this fact.

6.4. The Vandermonde Construction

Let A be a finite chain ring and let the integer m be a unit in A. (This means, in particular, that m is relatively prime to the characteristic of A.) Suppose that A contains a unit ζ of order m. Then the polynomial $Y^m - 1$ splits completely into linear factors:

$$Y^m - 1 = (Y - 1)(Y - \zeta) \cdots (Y - \zeta^{m-1}).$$

From the Fourier Transform of Section 5, we see that if we write

$f = f_0 + f_1 Y + \cdots + f_{m-1} Y^{m-1} \in A[Y]/(Y^m - 1)$, where $f_i \in A$ for $0 \leq i \leq m-1$, then

$$\begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{m-1} \end{pmatrix} = V^{-1} \begin{pmatrix} \hat{f}_0 \\ \hat{f}_1 \\ \vdots \\ \hat{f}_{m-1} \end{pmatrix},$$

where $\hat{f}_i$ are the Fourier coefficients and $V = \left(\zeta^{ij}\right)_{0 \leq i,j \leq m-1}$ is the $m \times m$ Vandermonde matrix.

For a given positive integer ℓ, let $\mathbf{a}_0, \ldots, \mathbf{a}_{m-1} \in A^\ell$ be m vectors. The construction

$$V^{-1} \begin{pmatrix} \mathbf{a}_0 \\ \vdots \\ \mathbf{a}_i \\ \vdots \end{pmatrix}$$

gives an element of R^ℓ. If C_i $(0 \leq i \leq m-1)$ are linear codes over A of length ℓ, and $\mathbf{a}_i \in C_i$ for $0 \leq i \leq m-1$, then we obtain a linear code over R of length ℓ, which then corresponds to a quasi-cyclic code over A of length ℓm and of index ℓ.

One sees readily that the above construction gives exactly the Vandermonde product defined in [15, Chapter 8]. We therefore obtain the following theorem:

THEOREM 6.4. *Let A be a finite chain ring, let m be an integer that is a unit in A and suppose that A contains a unit of order m. Let $C_0, \ldots, C_{m-1}$ be linear codes of length ℓ over A. Then the Vandermonde product of $C_0, \ldots, C_{m-1}$ is a quasi-cyclic code over A of length ℓm and of index ℓ. Moreover, when A and m are as above, every ℓ-quasi-cyclic code of length ℓm over A is obtained via the Vandermonde construction.*

7. Codes Over $\mathbf{Z}_{2k}$

(Exceptionally in this section, the base ring is not local). Recall that a self-dual code over $\mathbf{Z}_{2k}$ is of Type II if and only if the Euclidean weight of each of its codewords is a multiple of $4k$ (cf. [1, Section II]).

Although the ring $\mathbf{Z}_{2k}$ is not local, the decomposition (1) due to the Chinese Remainder Theorem still holds in some cases. Let $2k = p_1^{e_1} \ldots p_r^{e_r}$ be the prime power factorization of $2k$, where $p_1, \ldots, p_r$ are distinct primes. We first note that, for any $f \in \mathbf{Z}_{2k}[Y]$,

$$\frac{\mathbf{Z}_{2k}[Y]}{(f)} = \frac{\mathbf{Z}_{p_1^{e_1}}[Y]}{(f)} \times \cdots \times \frac{\mathbf{Z}_{p_r^{e_r}}[Y]}{(f)}. \tag{7}$$

Since $Y^2 + Y + 1$ is irreducible modulo 2, it follows that $Y^2 + Y + 1$ is irreducible modulo $2k$ for all positive integers k. Suppose k is relatively prime to 3. Then 3 is a unit in $\mathbf{Z}_{p_i^{e_i}}$ for every $1 \leq i \leq r$. Hence $Y - 1$ and $Y^2 + Y + 1$ are relatively prime in $\mathbf{Z}_{p_i^{e_i}}[Y]$, as

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

In particular, the Chinese Remainder Theorem implies that

$$\frac{\mathbf{Z}_{p_i^{e_i}}[Y]}{(Y^3 - 1)} = \mathbf{Z}_{p_i^{e_i}} \oplus \frac{\mathbf{Z}_{p_i^{e_i}}[Y]}{(Y^2 + Y + 1)}, \tag{8}$$

for every $1 \leq i \leq r$. Equations (7) (with $f(Y) = Y - 1$) and (8) together imply

$$\frac{\mathbf{Z}_{2k}[Y]}{(Y^3 - 1)} = \mathbf{Z}_{2k} \oplus \frac{\mathbf{Z}_{2k}[Y]}{(Y^2 + Y + 1)}.$$

Hence, for k relatively prime to 3, an ℓ-quasi-cyclic code of length 3ℓ over $\mathbf{Z}_{2k}$ can be regarded as corresponding to the pair (C_1, C_2), where C_1 is a code of length ℓ over $\mathbf{Z}_{2k}$ and C_2 is a code of length ℓ over $\mathbf{Z}_{2k}[Y]/(Y^2 + Y + 1)$. As in the case of binary codes, we call C_1 the $\mathbf{Z}_{2k}$-component of C.

PROPOSITION 7.1. *Let k be an integer coprime with 3 and let C be a self-dual code over $\mathbf{Z}_{2k}$. Then C is a Type II ℓ-quasi-cyclic code of length 3ℓ if and only if its $\mathbf{Z}_{2k}$ component C_1 is of Type II.*

Proof. The condition is necessary because C contains $(\mathbf{x}, \mathbf{x}, \mathbf{x})$, where $\mathbf{x}$ ranges over C_1, and, by hypothesis, $(4k, 3) = 1$.

The condition is sufficient because a spanning set of codewords of Euclidean weights $\equiv 0 \bmod 4k$ is

$$(\mathbf{x}, \mathbf{x}, \mathbf{x}), (-\mathbf{a}, \mathbf{b}, \mathbf{a} - \mathbf{b}),$$

with $\mathbf{x}$ running over C_1, and $\mathbf{a} + \zeta\mathbf{b}$ running over C_2. Observe that the self-duality of C_2 entails that $(\mathbf{a} + \zeta\mathbf{b})(\mathbf{a} + \overline{\zeta}\mathbf{b}) = 0$. Since

$$\zeta + \overline{\zeta} = -1 \quad \text{and} \quad \zeta\overline{\zeta} = 1,$$

we obtain therefrom

$$\mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} - \mathbf{a} \cdot \mathbf{b} \equiv 0 \bmod 2k.$$

Using the bilinearity of $(\cdot)$ as in

$$(\mathbf{a} - \mathbf{b}) \cdot (\mathbf{a} - \mathbf{b}) = \mathbf{a} \cdot \mathbf{a} + \mathbf{b} \cdot \mathbf{b} + 2\mathbf{a} \cdot \mathbf{b},$$

we obtain the norm of $(-\mathbf{a}, \mathbf{b}, \mathbf{a}-\mathbf{b})$ as

$$\mathbf{a}\cdot\mathbf{a}+\mathbf{b}\cdot\mathbf{b}+(\mathbf{a}-\mathbf{b})\cdot(\mathbf{a}-\mathbf{b}) = 2(\mathbf{a}\cdot\mathbf{a}+\mathbf{b}\cdot\mathbf{b}-\mathbf{a}\cdot\mathbf{b}),$$

which is therefore a multiple of $4k$. ∎

For instance, a putative extremal $\mathbf{Z}_8$-code of Type II of length 72 would have for $\mathbf{Z}_8$ component an extremal $\mathbf{Z}_8$-code of Type II of length 24.

8. Conclusion

In this work we have shown that all quasi-cyclic codes admitted some sort of combinatorial construction from codes of lower lengths. A new quaternary construction of the Leech lattice is also derived.

A. Appendix

A.1. Algebraic Characterization

In this appendix we describe a group-theoretic approach to quasi-cyclic codes. Throughout this section, the code C is defined over any finite commutative ring A. Recall that the permutation group $Perm(C)$ of a code C of length n is the subgroup of S_n, the group of all permutations on n letters, that fixes C under coordinate permutations. We begin with a characterization of quasi-cyclic codes in terms of permutation groups.

PROPOSITION A.1. *A code C of length $n = \ell m$ is ℓ-quasi-cyclic if and only if $Perm(C)$ contains a fixed point free (fpf) permutation consisting of ℓ disjoint m-cycles. In particular, if p denotes a prime, C of length $n = \ell p$ is ℓ-quasi-cyclic if and only if $Perm(C)$ contains an fpf permutation of order p.*

Proof. If C is ℓ-quasi-cyclic, then T^ℓ is the permutation sought for, where T denotes the cyclic shift. Conversely, if $Perm(C)$ contains such a permutation σ, then up to coordinate labeling, we can assume that $\sigma = T^\ell$. ∎

For the sake of illustration, recall that the affine group $\mathrm{Aff}(q)$ acts on $\mathbf{F}_q$ by transformations of the type $x \mapsto ax+b$ with a, b in $\mathbf{F}_q$ and a nonzero. A code of length q is called affine invariant if its permutation group contains $\mathrm{Aff}(q)$. The chief examples of such codes are the extended BCH codes.

COROLLARY A.2. *Let C be an affine invariant code of length $q = p^s$, where p is a prime. Then C is ℓ-quasi-cyclic for $\ell = p^{s-1}$ and no other value of ℓ.*

Proof. It is straightforward to check that the only fpf permutations of $\mathrm{Aff}(q)$ are the translations $x \mapsto x + b$ with b nonzero which are of order p. ■

COROLLARY A.3. *Let C be a code of length $p+1$ invariant under $PSL(2, p)$, where p is a prime. Then C is 2ℓ-quasi-cyclic for every divisor 2ℓ of $(p+1)$.*

Proof. By [22, Chap. 16, Lemma 14], $Perm(C)$ contains an fpf permutation made of two disjoint cycles of length $(p+1)/2$. Therefore its $\ell =: (p+1)/2d$-th power is also fpf but of order d. By the characterization in Proposition A.1, the result follows. ■

Remark. When A is a finite field, examples of codes that satisfy the condition in Corollary A.3 are the extended quadratic residue codes.

A.2 $q = m = 2$ and the Squaring Construction

It is well-understood since Dougherty et al. [6] that the case $q = m = 2$ corresponds to binary image of codes over $\mathbf{F}_2 + u\mathbf{F}_2$. If the latter code is of multilevel type (i.e., $D_1 + uD_2$, where D_1 and D_2 are binary codes), then the former is equivalent to a code obtained from the nested $(\mathbf{u} \mid \mathbf{u} + \mathbf{v})$ construction (applied to the ordered pair (D_2, D_1) with $D_1 \subseteq D_2$). The nested construction is a special case of the twisted squaring construction [2].

PROPOSITION A.4. *A binary code is ℓ-quasi-cyclic of length 2ℓ if and only if it is the binary image of a code over $\mathbf{F}_2 + u\mathbf{F}_2$. That latter code is of multilevel type if and only if the former code is obtained from the nested squaring construction.*

Proof. By the characterization in Proposition A.1, being binary ℓ-quasi-cyclic of length 2ℓ is equivalent to admitting an fpf involutory permutation. The result follows by [6]. ■

A.3 $q = m = 3$ and the $(u + v + w \mid 2u + v \mid u)$ Construction

In Kschichang et al. [18], the following construction is introduced

$$KP(U, V, W) := \{(\mathbf{u} + \mathbf{v} + \mathbf{w} \mid 2\mathbf{u} + \mathbf{v} \mid \mathbf{u}) \mid \mathbf{u} \in U,\ \mathbf{v} \in V,\ \mathbf{w} \in W\},$$

where U, V, W are codes of the same length over some ring A. We say that such a construction is nested if the chain of inclusions $W \subseteq V \subseteq U$ holds. It is proved in loc. cit. that the minimum distance is

$$\min(3d_U, 2d_V, d_W),$$

where d_U, d_V, d_W denote the minimum distances of U, V, W respectively.

Define the chain ring $R27$ as $\mathbf{F}_3[Y]/(Y^3 - 1)$, or equivalently $\mathbf{F}_3 + u\mathbf{F}_3 + u^2\mathbf{F}_3$ with $u^3 = 0$. Define the Gray map as

$$\phi(\mathbf{a} + \mathbf{b}Y + \mathbf{c}Y^2) = (\mathbf{a}, \mathbf{b}, \mathbf{c}),$$

or equivalently,

$$\phi(\mathbf{r} + \mathbf{s}u + \mathbf{t}u^2) = (\mathbf{r} + \mathbf{s} + \mathbf{t}, 2\mathbf{t} + \mathbf{s}, \mathbf{t}).$$

PROPOSITION A.5. *A ternary code is ℓ-quasi-cyclic of length 3ℓ if and only if it is the ternary Gray image of an R27 code. That latter code is of multilevel type if and only if the former code is equivalent to a code obtained by the nested KP construction.*

Proof. To check the equivalence of the two definitions of the Gray map, let $u = Y - 1$. The first assertion follows by the characterization. The strong KP condition is needed to ensure $R27$-linearity in a multilevel construction. The second assertion follows. ■

For instance the $[12, 6, 6]$ ternary Golay code is 4-quasi-cyclic (its permutation group contains $PSL(2, 11)$) but cannot be obtained from a multilevel type code since then $d_W \leq 4$.

Acknowledgment

Part of this work was done when San Ling was visiting CNRS-I3S, ESSI, Sophia Antipolis, France.

San Ling would like to thank the institution for the kind hospitality. The research of San Ling is partially supported by MOE-ARF research grant R-146-000-029-112 and DSTA research grant R-394-000-011-422.

References

1. E. Bannai, S. T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices, and invariant rings, *IEEE Trans. Inform. Theory*, Vol. (45) (1999) pp. 1194–1205.
2. Y. Berger and Y. Béery, The twisted squaring construction trellis complexity, and generalized weights of BCH and QR codes, *IEEE Trans. Inform. Theory*, Vol. (42) (1996) pp. 1817–1827.
3. A. Bonnecaze, P. Solé and A. R. Calderbank, Quaternary quadratic residue codes and unimodular lattices, *IEEE Trans. Inform. Theory*, Vol. (41) (1995) pp. 366–377.
4. Z. Chen, http://www.tec.hkr.se/~chen/research/codes/
5. J. Conan and C. Séguin, Structural properties and enumeration of quasi-cyclic codes, *AAECC*, Vol. (4) (1993) pp. 25–39.
6. S. T. Dougherty, P. Gaborit, M. Harada and P. Solé, Type II codes over $\mathbf{F}_2 + u\mathbf{F}_2$, *IEEE Trans. Inform. Theory*, Vol. (45) (1999) pp. 32–45.
7. M. Esmaeili, T. A. Gulliver, N. P. Secord and S. A. Mahmoud, A link between quasi-cyclic codes and convolutional codes, *IEEE Trans. Inform. Theory*, Vol. (44) (1998) pp. 431–435.

8. W. Feit, A self-dual even $(96, 48, 16)$ code, *IEEE Trans. Inform. Theory*, Vol. (20) (1974) pp. 136–138.
9. G. D. Forney, Coset codes II: binary lattices, *IEEE Trans. Inform. Theory*, Vol. (34) (1988) pp. 1152–1187.
10. T. A. Gulliver and V. K. Bhargava, Some best rate $1/p$ and rate $(p-1)/p$ systematic quasi-cyclic codes, *IEEE Trans. Inform. Theory*, Vol. (37) (1991) pp. 552–555.
11. T. A. Gulliver and V. K. Bhargava, Nine good $(m-1)/pm$ quasi-cyclic codes, *IEEE Trans. Inform. Theory*, Vol. (38) (1992) pp. 1366–1369.
12. 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 Trans. Inform. Theory*, Vol. (38) (1992) pp. 1369–1374.
13. T. A. Gulliver and V. K. Bhargava, Twelve good rate $(m-r)/pm$ binary quasi-cyclic codes, *IEEE Trans. Inform. Theory*, Vol. (39) (1993) pp. 1750–1751.
14. W. C. Huffman, Codes and groups, In (V. S. Pless and W. C. Huffman eds.) *Handbook of Coding Theory, Vol. II*, Elsevier Science, Amsterdam (1998) pp. 1345–1440.
15. G. Hughes, Codes and arrays from cocycles, Ph.D. Thesis, Royal Melbourne Institute of Technology (2000).
16. G. Hughes, Constacyclic codes, cocycles and $a\,\mathbf{u}+\mathbf{v}\,|\,\mathbf{u}-\mathbf{v}$ construction, *IEEE Trans. Inform. Theory*, Vol. (46) (2000) pp. 674–680.
17. T. Kasami, A Gilbert-Varshamov bound for quasi-cyclic codes of rate 1/2, *IEEE Trans. Inform. Theory*, Vol. (20) (1974) p. 679.
18. F. K. Kschichang and S. Pasupathy, Some ternary and quaternary codes and associated sphere packings, *IEEE Trans. Inform. Theory*, Vol. (38) (1992) pp. 227–246.
19. K. Lally and P. Fitzpatrick, Algebraic structure of quasicyclic codes, *Disc. Appl. Math.*, Vol. (111) (2001) pp. 157–175.
20. 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.
21. S. Ling and P. Solé, On the algebraic structure of quasi-cyclic codes I: finite fields, *IEEE Trans. Inform. Theory*, Vol. (47) (2001) pp. 2751–2760.
22. F. J. MacWilliams, N. J. A. Sloane, *The Theory of Error Correcting Codes*, North-Holland (1977).
23. B. R. McDonald, *Finite rings with identity*, Marcel Dekker, New York (1974).
24. G. H. Norton and A. Salagean, On the Hamming distance of linear codes over a finite chain ring, *IEEE Trans. Inform. Theory*, Vol. (46) (2000) pp. 1060–1067.
25. G. H. Norton and A. Salagean, On the structure of linear and cyclic codes over a finite chain ring, *AAECC*, Vol. (10) (2000) pp. 489–506.
26. V. Pless, Symmetry codes over $GF(3)$ and new 5-designs, *J. Comb. Theory*, Vol. (12) (1972) pp. 119–142.
27. N. J. A. Sloane, S. M. Reddy and C.-L. Chen, New binary codes, *IEEE Trans. Inform. Theory*, Vol. (18) (1972) pp. 503–510.
28. N. J. A. Sloane and J. G. Thompson, Cyclic self-dual codes, *IEEE Trans. Inform. Theory*, Vol. (29) (1983) pp. 364–366.
29. G. Solomon and H. C. A. van Tilborg, A connection between block codes and convolutional codes, *SIAM J. Appl. Math.*, Vol. (37) (1979) pp. 358–369.
30. A. Vardy, Trellis structure of codes, In (V. S. Pless and W. C. Huffman eds.), *Handbook of Coding Theory, Vol. II*, Elsevier Science, Amsterdam (1998) pp. 1989–2118.
31. E. J. Weldon, Jr., Long quasi-cyclic codes are good, *IEEE Trans. Inform. Theory*, Vol. (16) (1970) p. 130.