This is the author's version of a work that was accepted for publication in Finite fields and their applications (Elsevier). Changes resulting from the publishing process, such as peer review, editing, corrections, structural formatting, and other quality control mechanisms may not be reflected in this document. Changes may have been made to this work since it was submitted for publication. A definitive version was subsequently published in Dougherty, ST, Fernández-Córdoba, C. and Ten-Valls, R. "Quasi-cyclic codes as cyclic codes over a family of local rings" in Finite fields and their applications, vol. 40 (July 2016), p. 138-149 DOI 10.1016/j.fja.2016.04.002

Quasi-Cyclic Codes as Cyclic Codes over a Family of Local Rings

Steven T. Dougherty,
Cristina Fernández-Córdoba,
and Roger Ten-Valls[*†‡§¶]

December 1, 2015

Abstract

We give an algebraic structure for a large family of binary quasi-cyclic codes. We construct a family of commutative rings and a canonical Gray map such that cyclic codes over this family of rings produce quasi-cyclic codes of arbitrary index in the Hamming space via the Gray map. We use the Gray map to produce optimal linear codes that are quasi-cyclic.

Key Words: Quasi-cyclic codes, codes over rings.

1 Introduction

Cyclic codes have been a primary area of study for coding theory since its inception. In many ways, they were a natural object of study since they have a natural algebraic description. Namely, cyclic codes can be described as ideals in a corresponding polynomial ring. A canonical algebraic description for quasi-cyclic codes has been more elusive. In this paper, we shall give an algebraic description of a large family of quasi-cyclic codes by viewing them as the image under a Gray map of cyclic codes over rings from a family which we describe. This allows for a construction of binary quasi-cyclic codes of arbitrary index.

[*]Manuscript received Month day, year; revised Month day, year.

[†]S. T. Dougherty is with the Department of Mathematics, University of Scranton, Scranton, PA 18510, USA (e-mail:prof.steven.dougherty@gmail.com).

[‡]C. Fernández-Córdoba is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: cristina.fernandez@uab.cat).

[§]R. Ten-Valls is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: roger.ten@uab.cat).

[¶]This work has been partially supported by the Spanish MEC grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

In [6], cyclic codes were studied over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ which give rise to quasi-cyclic codes of index 2. In [1], [2] and [3], a family of rings, $R_k = \mathbb{F}_2[u_1, u_2, \ldots, u_k]/\langle u_i^2 = 0\rangle$, was introduced. Cyclic codes were studied over this family of rings. These codes were used to produce quasi-cyclic binary codes whose index was a power of 2. In this work, we shall describe a new family of rings which contains the family of rings R_k. With this new family, we can produce quasi-cyclic codes with arbitrary index as opposed to simply indices that are a power of 2.

A code of length n over a ring R is a subset of R^n. If the code is also a submodule then we say that the code is linear. Let π act on the elements of R^n by $\pi(c_0, c_1, \ldots, c_{n-1}) = (c_{n-1}, c_0, c_1, \ldots, c_{n-2})$. Then a code C is said to be cyclic if $\pi(C) = C$. If $\pi^s(C) = C$ then the code is said to be quasi-cyclic of index s.

2 A Family of Rings

In this section, we shall describe a family of rings which contains the family of rings described in [1], [2] and [3].

Let $p_1, p_2, \ldots, p_t$ be prime numbers with $t \geq 1$ and $p_i \neq p_j$ if $i \neq j$, and let $\Delta = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}$. Let $\{u_{p_i,j}\}_{(1 \leq j \leq k_i)}$ be a set of indeterminants. Define the following ring

$$R_\Delta = R_{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}} = \mathbb{F}_2[u_{p_1,1}, \ldots, u_{p_1,k_1}, u_{p_2,1} \ldots, u_{p_2,k_2}, \ldots, u_{p_t,k_t}]/\langle u_{p_i,j}^{p_i} = 0\rangle,$$

where the indeterminants $\{u_{p_i,j}\}_{(1 \leq i \leq t, 1 \leq j \leq k_i)}$ commute. Note that for each Δ there is a ring in this family.

Any indeterminant $u_{p_i,j}$ may have an exponent in the set $J_i = \{0, 1, \ldots, p_i - 1\}$. For $\alpha_i \in J_i^{k_i}$ denote $u_{p_i,1}^{\alpha_{i,1}} \cdots u_{p_i,k_i}^{\alpha_{i,k_i}}$ by $u_i^{\alpha_i}$, and for a monomial $u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ in R_Δ we write u^α, where $\alpha = (\alpha_1, \ldots, \alpha_t) \in J_1^{k_1} \times \cdots \times J_t^{k_t}$. Let $J = J_1^{k_1} \times \cdots \times J_t^{k_t}$.

Any element c in R_Δ can be written as

$$c = \sum_{\alpha \in J} c_\alpha u^\alpha = \sum_{\alpha \in J} c_\alpha u_{p_1,1}^{\alpha_{1,1}} \cdots u_{p_1,k_1}^{\alpha_{1,k_1}} \cdots u_{p_t,1}^{\alpha_{t,1}} \cdots u_{p_t,k_t}^{\alpha_{t,k_t}}, \qquad (1)$$

with $c_\alpha \in \mathbb{F}_2$.

Lemma 2.1. *The ring R_Δ is a commutative ring with $|R_\Delta| = 2^{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}}$.*

Proof. The fact that the ring is commutative follows from the fact that the indeterminants commute.

There are $p_1^{k_1} \cdots p_t^{k_t}$ different values for $\alpha \in J$. Moreover, for each fixed α, we have that $c_\alpha \in \mathbb{F}_2$ and hence there are $2^{p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t}}$ elements in R_Δ. $\square$

We define the ideal $\mathfrak{m} = \langle u_{p_i,j} \rangle_{(1 \le i \le t, 1 \le j \le k_i)}$. We can write every element in R_Δ as $R_\Delta = \{a_0 + a_1 m \mid a_0, a_1 \in \mathbb{F}_2, m \in \mathfrak{m}\}$. We will prove that units of R_Δ are elements $a_0 + a_1 m$, with $m \in \mathfrak{m}$ and $a_0 \neq 0$. First, the following lemma is needed.

Lemma 2.2. *Let $m \in \mathfrak{m}$. There exists $\xi > 0$ such that $m^\xi \neq 0$ and $m^{\xi+1} = 0$.*

Proof. It is enough to prove that for $m \in \mathfrak{m}$ there exit ϵ such that $m^\epsilon = 0$; for example, it is true if $\epsilon = p_1 p_2 \cdots p_t$. Then it follows that there must be a minimal such exponent. □

Define the map $\mu : R_\Delta \to \mathbb{F}_2$, as $\mu(c) = c_{\mathbf{0}}$, where $c = \sum_{\alpha \in J} c_\alpha u^\alpha \in R_\Delta$ and $\mathbf{0}$ is the all-zero vector.

Lemma 2.3. *Let $c = \sum_{\alpha \in J} c_\alpha u^\alpha \in R_\Delta$. Then c is a unit if and only if $\mu(c) = 1$; that is, $c = 1 + m$, for $m \in \mathfrak{m}$.*

Proof. Consider $c = \sum_{\alpha \in J} c_\alpha u^\alpha \in R_\Delta$, and $A = \{\alpha \in J | c_\alpha = 1\}$.

If $c_{\mathbf{0}} = 0$, then define, $\beta_{i,j} = p_i - max_{\alpha \in A}(\alpha_{i,j})$, for $i = 1, \ldots, t$, $j = 1 \ldots, k_i$, and $\tilde{c} = u_1^{\beta_1} \cdots u_t^{\beta_t}$. We have that $c \cdot \tilde{c} = 0$ and therefore c is not a unit.

In the case when $c_{\mathbf{0}} = 1$, there exists $m \in \mathfrak{m}$ such that $c = 1 + m$. Consider the maximum ξ such that $m^\xi \neq 0$. We know such a ξ exists by Lemma 2.2. Then, $(1 + m)(1 + m + \cdots + m^\xi) = 1 + m^{\xi+1} = 1$. Therefore $c = 1 + m$ is a unit. □

As a natural consequence of the proof of the previous lemma, we have the following proposition.

Proposition 2.4. *For $m \in \mathfrak{m}$,*

$$(1 + m)^{-1} = 1 + m + \cdots + m^\xi,$$

where ξ is the maximum value such that $m^\xi \neq 0$.

Note that $\mu(m) = 0$ for $m \in \mathfrak{m}$. In fact, $\mathfrak{m} = Ker(\mu)$.

Lemma 2.5. *The ring R_Δ is a local ring, where the maximal ideal is $\mathfrak{m}$. Moreover $[R_\Delta : \mathfrak{m}] = 2$ and hence $R_\Delta / \mathfrak{m} \cong \mathbb{F}_2$.*

Proof. We have that $R_\Delta / Ker(\mu) \cong Im(\mu) = \mathbb{F}_2$. Therefore $[R_\Delta : \mathfrak{m}] = 2$ and $\mathfrak{m}$ is a maximal ideal.

If $\mathfrak{m}' \neq \mathfrak{m}$ is a maximal ideal, then there exits a unit $u \in \mathfrak{m}'$ which gives that $\mathfrak{m}' = R_\Delta$. Therefore $\mathfrak{m}$ is the unique maximal ideal. □

Now we will prove that R_Δ is in fact a Frobenious ring. To do that, first we shall determine the Jacobson radical and the socle of R_Δ. Recall that for a ring R, the Jacobson radical consists of all annihilators of simple left R-submodules. It can be characterized as the intersection of all maximal right ideals. Since R_Δ is a commutative local ring, we have that its Jacobson radical is:

$$Rad(R_\Delta) = \mathfrak{m} = \langle u_{p_i,j} \rangle_{(1 \le i \le t, 1 \le j \le k_i)}.$$

The socle of a ring R is defined as the sum of all the minimal one sided ideals of the ring. For the ring R_Δ there is a unique minimal ideal and hence the socle of the ring R_Δ is:

$$Soc(R_\Delta) = \{0, u_{p_1,1}^{p_1-1} \cdots u_{p_1,k_1}^{p_1-1} \cdots u_{p_t,1}^{p_t-1} \cdots u_{p_t,k_t}^{p_t-1}\}.$$

Note that the socle of R_Δ is, in fact, the annihilator of $\mathfrak{m}$, $Ann_{R_\Delta}(\mathfrak{m})$.

Theorem 2.6. *The local ring R_Δ is a Frobenius ring.*

Proof. With the definition of $Rad(R_\Delta)$ and $Soc(R_\Delta)$, we have that $R_\Delta/Rad(R_\Delta) = R_\Delta/\mathfrak{m} \cong \mathbb{F}_2 \cong Soc(\mathfrak{m})$ and hence R_Δ is a Frobenius ring. □

For a complete description of codes over Frobenius rings, see [7].

2.1 Codes over R_Δ and their Orthogonals

Recall that a linear code of length n over R_Δ is a submodule of R_Δ^n. We define the usual inner-product, namely

$$[\mathbf{w}, \mathbf{v}] = \sum w_i v_i \text{ where } \mathbf{w}, \mathbf{v} \in \mathcal{R}_\Delta^n.$$

The orthogonal of a code C is defined in the usual way as

$$C^\perp = \{\mathbf{w} \in \mathcal{R}_\Delta^n \mid [\mathbf{w}, \mathbf{v}] = 0, \ \forall \mathbf{v} \in C\}.$$

By Theorem 2.6, we have that R_Δ is a Frobenius ring and hence we have that both MacWilliams relations hold, see [7] for a complete description. This implies that we have at our disposal the main tools of coding theory to study codes over this family of rings. In particular, we have that $|C||C^\perp| = |{R_\Delta}^n| = 2^{\Delta n}$.

2.2 Ideals of R_Δ

In this subsection, we shall study some ideals in the ring R_Δ. We will see later in Theorem 5.5, the importance of understanding the ideal structure of R_Δ.

Let A_Δ be the set of all monomials of R_Δ and $\widehat{A}_\Delta$ be the subset of A_Δ of all monomials with one indeterminant. Clearly $|A_\Delta| = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} = \Delta$

and $|\widehat{A}_\Delta| = p_1^{k_1}+p_2^{k_2}+\cdots+p_t^{k_t}$. View each element $a \in A_\Delta$, $a = u^\alpha$ for some $\alpha \in J$, as the subset $\{u_{p_i,j}^{\alpha_{i,j}} | \alpha_{i,j} \neq 0\}_{(1\leq i\leq t, 1\leq j\leq k_i)} \subseteq \widehat{A}_\Delta$. We will denote by $\widehat{a}$ the corresponding subset of $\widehat{A}_\Delta$. For example, the element $a = u_{2,1}u_{3,4}^2u_{5,2}^3$ is identified with the set $\widehat{a} = \{u_{2,1}, u_{3,4}^2, u_{5,2}^3\}$. Note that $1 \in A_\Delta$ and $\widehat{1} = \emptyset$, the empty set.

Consider the vector of exponents $\alpha = (\alpha_{1,1}, \ldots, \alpha_{1,k_1}, \ldots, \alpha_{t,1}, \ldots, \alpha_{t,k_t}) \in J$ and denote by $\bar{\alpha}$ the vector $(p_1 - \alpha_{1,1}, \cdots, p_1 - \alpha_{1,k_1}, \cdots, p_t - \alpha_{t,k_t})$, note that $\bar{\bar{\alpha}} = \alpha$.

Let I_α be the ideal $I_\alpha = \langle u^\alpha \rangle$, for $\alpha \in J$. Note that $I_{\mathbf{0}} = \langle 1 \rangle = R_\Delta$. We also define $I_{(p_1,\cdots,p_1,p_2\cdots,p_t,\cdots,p_t)} = \{0\}$. Now we define the ideal

$$\widehat{I}_\alpha = \langle \widehat{u^\alpha} \rangle = \langle u_{p_i,j}^{\alpha_{i,j}} \mid \alpha_{i,j} \neq 0 \rangle_{(1\leq i\leq t, 1\leq j\leq k_i)}.$$

Example 1. *Consider* $\Delta = 3^2 5$ *and* $\alpha = (2, 1, 2)$. *Then with the previous definitions,* $I_\alpha = \langle u_{3,1}^2 u_{3,2} u_{5,1}^2 \rangle$, $\widehat{I}_\alpha = \langle u_{3,1}^2, u_{3,2}, u_{5,1}^2 \rangle$, *and* $I_{\bar{\alpha}} = \langle u_{3,1} u_{3,2}^2 u_{5,1}^3 \rangle$. *Note that* $\langle u_{3,1}^2, u_{3,2}, u_{5,1}^2 \rangle^\perp = \langle u_{3,1} u_{3,2}^2 u_{5,1}^3 \rangle$. *The following proposition will prove this fact in general.*

Proposition 2.7. *Let* $\alpha \in J$ *be a vector of exponents. Then* $\widehat{I}_\alpha^\perp = I_{\bar{\alpha}}$.

Proof. It is clear that $I_{\bar{\alpha}} \subset \widehat{I}_\alpha^\perp$. Then we are going to see that $\widehat{I}_\alpha^\perp \subset I_{\bar{\alpha}}$. Suppose that it is not true, then there exist an element $b = \sum_{\beta\in J} c_\beta u^\beta \in \widehat{I}_\alpha^\perp$ that does not belong to $I_{\bar{\alpha}}$. Then there exists a particular β such that $c_\beta \neq 0$ and $\beta_{i,j} < \bar{\alpha}_{i,j}$ for some i and j. Then, $u_{p_i,j}^{\alpha_{i,j}} \cdot b \neq 0$ for $u_{p_i,j}^{\alpha_{i,j}} \in \widehat{I}_\alpha$. Therefore, $b \notin \widehat{I}_\alpha^\perp$ and $\widehat{I}_\alpha^\perp \subset I_{\bar{\alpha}}$. □

Here, we have $\widehat{I}_{\mathbf{0}}^\perp = R_\Delta^\perp = \{0\} = I_{(p_1,\cdots,p_1,p_2\cdots,p_t,\cdots,p_t)} = I_{\bar{\mathbf{0}}}$.

Proposition 2.8. *The number of elements of* I_α *is* $2^{\prod_{i\in\bar{\alpha}} i}$ *and the number of elements of* $\widehat{I}_\alpha$ *is* $2^{\Delta-\prod_{i\in\alpha} i}$.

Proof. Consider the set of all monomials of I_α. There are $p_1 - \alpha_{1,1}$ different monomials fixing all the indeterminates except the first one, $u_{p_1,1}$. There are $p_1 - \alpha_{1,2}$ different monomials fixing all the indeterminates except the second one, $u_{p_1,2}$. By induction and by the laws of counting, there are $\prod_{1\leq i\leq t, 1\leq j\leq k_i}(p_i - \alpha_{i,j})$ different monomials in I_α. Since $\bar{\alpha}$ is the vector $(p_1 - \alpha_{1,1}, \cdots, p_1 - \alpha_{1,k_1}, \cdots, p_t - \alpha_{t,k_t})$ and all element in I_α are a linear combination of its monomials, we have that $|I_\alpha| = 2^{\prod_{i\in\bar{\alpha}} i}$. By Proposition 2.7, clearly we have that $|\widehat{I}_\alpha| = 2^{\Delta-\prod_{i\in\alpha} i}$. □

Example 2. *We continue Example 1 by counting the size of the ideals given there. We note that* $\Delta = 45$. *Here* $\alpha = (2, 1, 2)$ *and so* $\overline{\alpha} = (1, 2, 3)$. *Then* $|I_\alpha| = 2^6 = 64$ *and* $|\widehat{I}_\alpha| = 2^{45-4} = 2^{41} = 2,199,023,255,552$.

3 Gray map to the Hamming Space

We will consider the elements in R_Δ as a binary vector of Δ coordinates and consider the set A_Δ. Order the elements of A_Δ lexicographically and use this ordering to label the coordinate positions of $\mathbb{F}_2^\Delta$. For $a \in A_\Delta$, define the Gray map $\Psi : R_\Delta \to \mathbb{F}_2^\Delta$ as follows:

For all $b \in A_\Delta$

$$\Psi(a)_b = \begin{cases} 1 & \text{if } \widehat{b} \subseteq \{\widehat{a} \cup 1\}, \\ 0 & \text{otherwise,} \end{cases}$$

where $\Psi(a)_b$ indicates the coordinate of $\Psi(a)$ corresponding to the position of the element $b \in A_\Delta$ with the defined ordering. We have that $\Psi(a)_b$ is 1 if each indeterminant $u_{p_i,j}$ in the monomial b with non-zero exponent is also in the monomial a with the same exponent; that is, $\bar{b}$ is a subset of $\bar{a}$. In order to consider all the subsets of $\bar{a}$, we also add the empty subset that is given when $b = 1$; that is we compare $\bar{b}$ to $\widehat{a} \cup 1$. Then extend Ψ linearly for all elements of R_Δ.

Example 3. *Let $\Delta = 6 = 2 \cdot 3$, then we have the following ordering of the monomials $[1, u_{2,1}, u_{2,1}u_{3,1}, u_{2,1}u_{3,1}^2, u_{3,1}, u_{3,1}^2]$. As examples,*

$$\Psi(1) = (1,0,0,0,0,0), \qquad \Psi(u_{3,1}^2) = (1,0,0,0,0,1),$$
$$\Psi(u_{2,1}u_{3,1}) = (1,1,1,0,1,0), \quad \Psi(u_{2,1}u_{3,1}^2) = (1,1,0,1,0,1).$$

Proposition 3.1. *Let $a \in A_\Delta$ such that $a \neq 1$. Then $wt_H(\Psi(a))$ is even.*

Proof. Since $\widehat{a}$ is a non-empty set then $\widehat{a}$ has $2^{|\widehat{a}|}$ subsets. Thus, $\Psi(a)$ has an even number of non-zero coordinates. □

Notice that for $a, b \in A_\Delta$ such that $a, b \neq 1$, we have

$$wt_H(\Psi(a+b)) = wt_H(\Psi(a)) + wt_H(\Psi(b)) - 2wt_H(\Psi(a) \star \Psi(b))),$$

which is even, where $\star$ is the componentwise product. Therefore we have the following result.

Theorem 3.2. *Let m be an element of R_Δ. Then, $m \in \mathfrak{m}$ if and only if $wt_H(\Psi(m))$ is even.*

Proof. We showed that if $m \in \mathfrak{m}$ then $wt_H(\Psi(m))$ is even. Since $|\mathfrak{m}| = \frac{|R_\Delta|}{2}$ and there are precisely $|\mathfrak{m}| = \frac{|R_\Delta|}{2}$ binary vectors in $\mathbb{F}_2^\Delta$ of even weight, then the odd weight vectors correspond to the units in R_Δ. □

Each code C corresponds to a binary linear code, namely the code $\Psi(C)$ of length Δn. It is natural now to ask if orthogonality is preserved over the map Ψ. In the following case, as proven in [1], it is preserved as in the following proposition. Recall that the ring R_k was a special case of R_Δ when Δ was a power of 2.

Proposition 3.3. *Let $\Delta = 2^k$ and let C a linear code over R_Δ of length n. Then,*

$$\Psi(C^\perp) = (\Psi(C))^\perp.$$

In general, orthogonality will not be preserved. In the next example we will see that if C is a code over R_Δ then, in general, $\Psi(C)^\perp \neq \Psi(C^\perp)$ and the following diagram does not commute:

$$\begin{array}{ccc} C & \xrightarrow{\Psi} & \Psi(C) \\ \downarrow & & \\ C^\perp & \xrightarrow{\Psi} & \Psi(C^\perp) \end{array}$$

Example 4. *Let $\Delta = 6 = 2 \cdot 3$ and consider the length one code $\widehat{I}_{(1,2)} = \langle u_{2,1}, u_{3,1}^2 \rangle$. By Proposition 2.7, we have that the dual is $\widehat{I}_{(1,2)}^\perp = I_{(1,1)} = \langle u_{2,1}u_{3,1} \rangle$. Clearly, $[u_{3,1}^2, u_{2,1}u_{3,1}] = 0 \in R_\Delta$ but, by Example 3, we have that $[\Psi(u_{3,1}^2), \Psi(u_{2,1}u_{3,1})] \neq 0$.*

Computing $\Psi(\widehat{I}_{(1,2)})^\perp$ and $\Psi(\widehat{I}_{(1,2)}^\perp)$ one obtains binary linear codes with parameters $[6, 2, 2]$ and $[6, 2, 4]$, respectively. That is, not only are they different codes but they have different minimum weights and hence not equivalent.

4 MacWilliams Relations

Let C be a linear code over R_Δ of length n. Define the complete weight enumerator of C in the usual way, namely:

$$cwe_C(X) = \sum_{c \in C} \prod_{i=1}^{n} x_{c_i}.$$

We are using X to denote the set of variables (x_{c_i}) where the c_i are the elements of R_Δ in some order.

In order to relate the complete weight enumerator of C with the complete weight enumerator of its dual, we first shall define a generator character of the ring. It is well known, see [7], that a finite ring is Frobenius if and only if it admits a generating character. Hence, a generating character exits for the ring R_Δ. We shall find this character explicitly.

Define the character $\chi : R_\Delta \longrightarrow \mathbb{C}^\star$ as

$$\chi(\sum_{\alpha \in J} c_\alpha u^\alpha) = \prod_{\alpha \in J} (-1)^{c_\alpha}.$$

In other words, the character has a value of -1 if there are oddly many monomials and 1 if there are evenly many monomials in a given element.

Consider the minimal ideal of the ring

$$Soc(R_\Delta) = \{0, u_{p_1,1}^{p_1-1} \cdots u_{p_1,k_1}^{p_1-1} \cdots u_{p_t,1}^{p_t-1} \cdots u_{p_t,k_t}^{p_t-1}\}.$$

Note that $\chi(0) = 1$ and $\chi(u_{p_t,1}^{p_t-1} \cdots u_{p_t,k_t}^{p_t-1}) = -1$ since it is a single monomial. Therefore, χ is non-trivial on the minimal ideal. Note also that this minimal ideal is contained in all ideals of the ring R_Δ since it is the unique minimal ideal. This gives that $ker(\chi)$ contains no non-trivial ideal. Hence, by Lemma 4.1 in [7], we have that the character χ is a generating character of the ring R_Δ. This generating character allows us to give the MacWilliams relations explicitly.

Use the elements of R_Δ as coordinates for the rows and columns. Let T be the $|R_\Delta| \times |R_\Delta|$ matrix given by $T_{a,b} = \chi(ab)$, for $a, b \in R_\Delta$. By the results in [7], we have the following theorem.

Theorem 4.1. *Let C be a linear code over R_Δ. Then*

$$cwe_{C^\perp}(X) = \frac{1}{|C|} cwe_C(T \cdot X),$$

where $T \cdot X$ represents the action of T on the vector X given by matrix multiplication TX^t, where X^t is the transpose of X.

5 Cyclic codes over R_Δ

In this section, we shall give an algebraic description of cyclic codes over R_Δ. These codes will, in turn, give quasi-cyclic codes of index Δ over $\mathbb{F}_2$.

Recall that, for an element a in R_Δ, $\mu(a)$ is the reduction modulo $\{u_{p_i,j}\}$ for all $i \in \{1, \ldots, t\}$ and $j \in \{1, \ldots, k_i\}$. Now, we can define a polynomial reduction μ from $R_\Delta[x]$ to $\mathbb{F}_2[x]$ where $\mu(f) = \mu(\sum a_i x^i) = \sum \mu(a_i) x^i$.

A monic polynomial f over $R_\Delta[x]$ is said to be a basic irreducible polynomial if $\mu(f)$ is an irreducible polynomial over $\mathbb{F}_2[x]$. Since $\mathbb{F}_2$ is a subring of R_Δ then, any irreducible polynomial in $\mathbb{F}_2[x]$ is a basic irreducible polynomial viewed as a polynomial of $R_\Delta[x]$.

Lemma 5.1. *Let n be an odd integer. Then, $x^n - 1$ factors into a product of finitely many pairwise coprime basic irreducible polynomials over R_Δ, $x^n - 1 = f_1 f_2 \ldots f_r$. Moreover, $f_1, f_2, \ldots, f_r$ are uniquely determined up to a rearrangement.*

Proof. The field $\mathbb{F}_2$ is a subring of R_Δ and $x^n - 1$ factors uniquely as a product of pairwise coprime irreducible polynomials in $\mathbb{F}_2[x]$. Therefore, the polynomial factors in R_Δ since $\mathbb{F}_2$ is a subring of R_Δ. Then Hensel's Lemma gives that regular polynomials (namely, polynomials that are not zero divisors) over R_Δ have a unique factorization. □

The previous lemma is highly dependent upon the fact that $\mathbb{F}_2$ is a subring of the ambient ring. Were this not the case, the lemma would not hold.

As in any commutative ring we can identify cyclic codes with ideals in a corresponding polynomial ring. We give the standard definitions to assign notation. Let $R_{\Delta,n} = R_\Delta[x]/\langle x^n - 1\rangle$.

Theorem 5.2. *Cyclic codes over R_Δ of length n can be viewed as ideals in $R_{\Delta,n}$.*

Proof. We view each codeword $(c_0, c_1, \dots, c_{n-1})$ as a polynomial $c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}$ in $R_{\Delta,n}$ and multiplication by x as the cyclic shift and the standard proof applies. □

The next theorem follows from the cannonical decomposition of rings, noting that for odd n the factorization is unique.

Theorem 5.3. *Let n be an odd integer and let $x^n - 1 = f_1f_2 \dots f_r$. Then, the ideals in $R_{\Delta,n}$ can be written as $I \cong I_1 \oplus I_2 \oplus \cdots \oplus I_r$ where I_i is an ideal of the ring $R_\Delta[x]/\langle f_i\rangle$, for $i = 1, \dots, r$.*

Let f be an irreducible polynomial in $\mathbb{F}_2[x]$, then f is a basic monic irreducible polynomial over R_Δ. Our goal now is to show that there is a one to one correspondence between ideals of $R_\Delta[x]/\langle f\rangle$ and ideals of R_Δ. We have that $\mathbb{F}_2[x]/\langle f\rangle$ is a finite field of order $2^{\deg(f)}$. Let $L_{0,0} = \mathbb{F}_2[x]/\langle f\rangle$ and $L_{p_1,1} = L_{0,0}[u_{p_1,1}]/\langle u_{p_1,1}^{p_1}\rangle$. For $1 \le i \le t, 1 \le j \le k_i$, define

$$L_{p_i,j} = \begin{cases} L_{p_{i-1},k_{i-1}}[u_{p_i,1}]/\langle u_{p_i,1}^{p_i}\rangle & \text{if } j = 1, \\ L_{p_i,j-1}[u_{p_i,j}]/\langle u_{p_i,j}^{p_i}\rangle & \text{otherwise.} \end{cases}$$

Then we have that any element $a \in L_{p_i,j}$ can be written as $a = a_0 + a_1u_{p_i,j} + a_2u_{p_i,j}^2 + \cdots + a_{p_i-1}u_{p_i,j}^{p_i-1}$ where $a_0, \dots, a_{p_i-1}$ belong to $L_{p_i,j-1}$ if $j \ne 1$ or to $L_{p_{i-1},k_{i-1}}$ if $j = 1$.

Proposition 5.4. *Let $a = \sum_{d=0}^{p_i-1} a_du_{p_i,j}^d$ be an element of $L_{p_i,j}$. Then, a is a unit in $L_{p_i,j}$ if and only if a_0 is a unit in $L_{p_i,j-1}$ if $j \ne 1$ or in $L_{p_{i-1},k_{i-1}}$ if $j = 1$.*

Proof. Suppose a_0 a unit in $L_{p_i,j-1}$ if $j \ne 1$ or in $L_{p_{i-1},k_{i-1}}$ if $j = 1$. Define $b = a_0^{-1}(\sum_{d=1}^{p_i-1} a_du_{p_i,j}^d)$. Clearly, b is a zero divisor and $1 + b$ is a unit since $(1 + b)(1 + b + b^2 + \cdots + b^{p_i-1}) = 1$. So $a_0(1 + b) = a$ is also a unit.

If a_0 is not a unit then there exists b in $L_{p_i,j-1}$ if $j \ne 1$ or in $L_{p_{i-1},k_{i-1}}$ if $j = 1$, such that $ba_0 = 0$. Therefore, $bu_{p_i,j}^{p_i-1}a = 0$. □

Denote by $\mathcal{U}(L_{p_i,j})$ the group of units of $L_{p_i,j}$. By the previous result we can see that

$$|\mathcal{U}(L_{p_i,j})| = \begin{cases} |\mathcal{U}(L_{p_{i-1},k_{i-1}})||L_{p_{i-1},k_{i-1}}| & \text{if } j = 1, \\ |\mathcal{U}(L_{p_i,j-1})||L_{p_i,j-1}| & \text{otherwise.} \end{cases}$$

Since $|\mathcal{U}(L_{0,0})| = 2^{\deg(f)} - 1$, we get that $|\mathcal{U}(L_{p_1,1})| = 2^{\deg(f)}(2^{\deg(f)} - 1)$. By induction, we obtain that

$$|L_{p_t,k_t}| = (2^{\deg(f)})^{\Delta} \text{ and } |\mathcal{U}(L_{p_t,k_t})| = (2^{\deg(f)})^{\Delta} - (2^{\deg(f)})^{\Delta-1}.$$

Moreover, the group $\mathcal{U}(L_{p_i,j})$ is the direct product of a cyclic group G of order $2^{deg(f)-1}$ and an abelian group H of order $(2^{deg(f)})^{\Delta-1}$.

Theorem 5.5. *The ideals of L_{p_t,k_t} are in bijective correspondence with the ideals of R_Δ.*

Proof. From Proposition 5.4, it is straightforward that the zero-divisors of L_{p_t,k_t} are of the form $\sum c_\alpha u_1^{\alpha_1} \cdots u_t^{\alpha_t}$ with $c_\alpha \in L_{0,0}$ and $c_{\mathbf{0}} = 0$, furthermore there are $(2^{\deg(f)})^{\Delta-1}$ of them. This gives the result. □

Corollary 5.6. *Let n be an odd integer. Let $x^n - 1 = f_1 f_2 \dots f_r$ be the factorization of $x^n - 1$ into basic irreducible polynomials over R_Δ and let I_Δ be the number of ideals in R_Δ. Then, the number of linear cyclic codes of length n over R_Δ is $(I_\Delta)^r$.*

6 One generator cyclic codes

We shall examine codes that have a single generator. We shall proceed in a similar way as was done in [2] for the case when Δ was a power of 2. If a polynomial $s \in R_{\Delta,n}$ generates an ideal, then the ideal is the entire space if and only if s is a unit. Hence we need to consider codes generated by a non-unit. For foundational results in this section, see [5].

Let $\mathfrak{C}_n$ denote the cyclic group of order n. Consider the group ring $R_\Delta \mathfrak{C}_n$. This ring is canonically isomorphic to $R_{\Delta,n}$. Any element in $R_\Delta \mathfrak{C}_n$ corresponds to a circulant matrix in the following form:

$$\sigma(a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_1 & a_2 & a_2 & \dots & a_0 \end{pmatrix}.$$

Take the standard definition of the determinant function, $det : M_n(R_\Delta) \to R_\Delta$.

Proposition 6.1. *An element $\alpha = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} \in R_{\Delta,n}$ is a non-unit if and only if $det(\sigma(\alpha)) \in \mathfrak{m}$. Equivalently, we have an element $\alpha = a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1}x^{n-1} \in R_{\Delta,n}$ is a non-unit if and only if $\mu(det(\sigma(\alpha))) = 0$.*

This proposition allows for a straightforward computational technique to find generators for cyclic codes over R_Δ which give binary quasi-cyclic codes of index Δ via the Gray map.

7 Binary Quasi-Cyclic Codes

In this section, we shall give an algebraic construction of binary quasi-cyclic codes from codes over R_Δ.

Lemma 7.1. *Let* $\mathbf{v}$ *be a vector in* R_Δ^n*. Then* $\Psi(\pi(\mathbf{v})) = \pi^\Delta(\Psi(\mathbf{v}))$.

Proof. The result is a direct consequence from the definition of Ψ. □

The following theorems gives a construction of linear binary quasi-cyclic codes of arbitrary index from cyclic codes and quasi-cyclic codes over R_Δ.

Theorem 7.2. *Let* C *be a linear cyclic code over* R_Δ *of length* n*. Then* $\Psi(C)$ *is a linear binary quasi-cyclic code of length* Δn *and index* Δ.

Proof. Since C is a cyclic code, $\pi(C) = C$. Then by Lemma 7.1, $\Psi(C) = \Psi(\pi(C)) = \pi^\Delta(\Psi(C))$. Hence $\Psi(C)$ is a quasi-cyclic code of index Δ. □

Theorem 7.3. *Let* C *be a linear quasi-cyclic code over* R_Δ *of length* n *and index* k*. Then,* $\Psi(C)$ *is a linear binary quasi-cyclic code of length* Δn *and index* Δk.

Proof. We can apply the same argument as in Theorem 7.2, taking into account that $\Psi(C) = \Psi(\pi^k(C)) = \pi^{\Delta k}(\Psi(C))$. □

8 Examples R_Δ

Examples of R_Δ-cyclic codes of length n for the case $\Delta = 2^{k_1}$ can be found in [2].

Table 1 shows some examples of one generator R_Δ-cyclic codes, for $\Delta \neq 2^{k_1}$, whose binary image via the Ψ map give optimal codes ([4]) with minimum distance at least 3. For each cyclic code $C \in \mathcal{R}_\Delta^n$, in the table there are the parameters $[\Delta, n]$, the generator polynomial, and the parameters $[N, k, d]$ of $\Psi(C)$, where N is the length, k is the dimension, and d is the minimum distance.

References

[1] S.T. Dougherty, B. Yildiz, and S. Karadeniz, Codes over R_k, Gray maps and their Binary Images, Finite Fields Appl., **17**, no. 3, 205 - 219, 2011.

[2] S.T. Dougherty, B. Yildiz, and S. Karadeniz, Cyclic Codes over R_k, Des. Codes Cryptog., **63**, no. 1, 113 - 126, 2012.

[3] S.T. Dougherty, B. Yildiz, and S. Karadeniz, Self-dual Codes over R_k and Binary Self-Dual Codes, Eur, J. of Pure and Appl. Math., **6**, no. 1, 2013.

[4] M. Grassl, Table of bounds on linear codes. http://www.codestable.de

[5] T. Hurley, Group Rings and Rings of Matrices, Inter. J. Pure and Appl. Math., **31**, no.3, 319 - 335, 2006.

[6] B. Yildiz, S. Karadeniz, Cyclic codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, Des. Codes Crypt., **54**, 61 - 81, 2011.

[7] Wood, Jay A. Duality for modules over finite rings and applications to coding theory. Amer. J. Math. **121**, no. 3, 555 - 575, 1999.

Table 1: Quasi-cyclic codes of index Δ

[Δ, n]	Generators	Binary Image
[6,2]	$(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2+u_{3,1})x+u_{2,1}u_{3,1}+u_{2,1}+u_{3,1}$	[12, 6, 4]
[6,3]	$(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1})x^2+(u_{2,1}u_{3,1}+u_{2,1}+u_{3,1})x$	[18, 11, 4]
[6,3]	$(u_{2,1}u_{3,1}^2+u_{2,1}+u_{3,1}^2+u_{3,1})x^2+(u_{2,1}u_{3,1}+u_{2,1}+u_{3,1})x$	[18, 10, 4]
[6,3]	$(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2)x^2+(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2)x$	[18, 4, 8]
[6,3]	$(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2)x^2+(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2)x+u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2$	[18, 2, 12]
[6,4]	$(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{2,1}+u_{3,1})x^3+(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1})x^2+(u_{2,1}u_{3,1}+u_{2,1}+u_{3,1})x$	[24, 8, 8]
[6,4]	$(u_{2,1}u_{3,1}^2+1)x^3+x^2+(u_{2,1}u_{3,1}+u_{2,1}+1)x+u_{2,1}u_{3,1}+u_{2,1}+1$	[24, 9, 8]
[6,6]	$(u_{2,1}u_{3,1}^2+u_{2,1}+u_{3,1}^2+1)x^5+(u_{3,1}^2+1)x^4+(u_{2,1}u_{3,1}^2+u_{2,1})x^3+(u_{2,1}+u_{3,1}^2+1)x^2+(u_{2,1}u_{3,1}+u_{2,1}+1)x$	[36, 17, 8]
[6,6]	$(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}+1)x^5+(u_{2,1}u_{3,1}^2+u_{2,1}u_{3,1}+u_{3,1}^2)x^4+(u_{2,1}u_{3,1}+u_{2,1}+u_{3,1}^2)x^3+(u_{2,1}u_{3,1}+u_{2,1}+1)x^2$	[36, 18, 8]
[6,7]	$(u_{2,1}u_{3,1}^2+u_{2,1}+u_{3,1}+1)x^6+(u_{2,1}u_{3,1}+u_{2,1}+u_{3,1}+1)x^5+(u_{2,1}u_{3,1}+u_{2,1}+1)x^4+(u_{2,1}u_{3,1}+u_{2,1}+1)x^2$	[42, 32, 4]
[6,7]	$(u_{2,1}+u_{3,1}+1)x^6+(u_{2,1}+u_{3,1}^2+1)x^5+(u_{3,1}^2+1)x^4+(u_{2,1}u_{3,1}+u_{3,1}^2+u_{3,1}x^3+(u_{2,1}u_{3,1}+u_{2,1}+1)x^2$	[42, 33, 4]
[9,2]	$(u_{3,1}^2u_{3,2}+u_{3,1}^2+u_{3,1}u_{3,2})x+u_{3,1}^2u_{3,2}^2+u_{3,1}^2u_{3,2}+u_{3,1}^2+u_{3,1}u_{3,2}$	[18, 4, 8]
[9,2]	$(u_{3,1}^2u_{3,2}^2+u_{3,1}^2+u_{3,1}u_{3,2}^2+u_{3,1}+1)x+u_{3,1}^2u_{3,2}+u_{3,1}u_{3,2}^2+u_{3,1}u_{3,2}+u_{3,1}+1$	[18, 10, 4]
[9,3]	$(u_{3,1}^2u_{3,2}+u_{3,1}^2+u_{3,1}u_{3,2}^2+u_{3,1}u_{3,2}+u_{3,1}+u_{3,2}^2+u_{3,2})x^2+(u_{3,1}^2+u_{3,1}u_{3,2}^2+u_{3,1}u_{3,2}+u_{3,1})x+u_{3,2}^2$	[27, 18, 4]
[9,4]	$(u_{3,1}^2u_{3,2}^2+u_{3,1}+u_{3,2}^2)x^3+(u_{3,1}^2+u_{3,1}+1)x^2+(u_{3,1}^2+u_{3,1}u_{3,2}^2+u_{3,1}u_{3,2}+u_{3,2}^2+1)x$	[36, 27, 4]
[12,3]	$(u_{2,1}u_{3,1}^2+u_{2,1}+u_{2,2}u_{3,1}^2+u_{2,2}u_{3,1}+u_{2,2}+u_{3,1}^2)x^2+(u_{2,1}u_{2,2}u_{3,1}^2+u_{2,1}u_{3,1}^2+u_{2,2}u_{3,1}+u_{2,2})x+u_{2,1}u_{2,2}u_{3,1}^2+u_{2,1}u_{2,2}+u_{2,1}u_{3,1}+u_{2,1}+u_{2,2}u_{3,1}^2+u_{2,2}u_{3,1}$	[36, 17, 8]
[12,3]	$u_{3,1}x^2+(u_{2,1}u_{2,2}u_{3,1}^2+u_{2,1}u_{3,1}^2+u_{2,2}u_{3,1}+u_{2,2})x+u_{2,1}u_{2,2}u_{3,1}^2+u_{2,1}u_{2,2}+u_{2,1}u_{3,1}+u_{2,1}+u_{2,2}u_{3,1}^2+u_{2,2}u_{3,1}$	[36, 18, 8]