Designs, Codes and Cryptography, 4, 145-155 (1994)
© 1994 Kluwer Academic Publishers. Manufactured in The Netherlands.

On Row-Cyclic Codes with Algebraic Structure*

ROBERTA EVANS SABIN
Computer Science Department, Loyola College, Baltimore, MD 21210-2699

Communicated by S. Vanstone
Received September 1, 1992; Revised June 22, 1993.

Abstract. In this article, some row-cyclic error-correcting codes are shown to be ideals in group rings in which the underlying group is metacyclic. For a given underlying group, several nonequivalent codes with this structure may be generated. Each is related to a cyclic code generated in response to the metrics associated with the underlying metacyclic group. Such codes in the same group ring are isomorphic as vector spaces but may vary greatly in weight distributions and so are nonequivalent. If the associated cyclic code is irreducible, examining the structure of its isomorphic finite field yields all nonequivalent codes with the desired structure. Several such codes have been found to have minimum distances equalling those of the best known linear codes of the same length and dimension.

1. Introduction

1.1. Quasi-Cyclic Codes

Let C, a linear (mn, k) block code over field F, have the positions of its symbols numbered $0, 1, \ldots, mn - 1$. Code C is considered row-cyclic (and quasi-cyclic) if it is invariant under permutations of its positions, i, of the form

$$\gamma_j : i \mapsto \big((i - i') + j\big) \bmod m + i' \text{ where } i' = \lfloor i/m \rfloor \cdot m \text{ and } 0 \le j < m \text{ [7].}$$

Consider a codeword of C to be a sequence of n elements of $F\mathbb{Z}_m$ where $\mathbb{Z}_m = <x>$. If C has a single generator g, where $g = \mid c_0(x) \mid c_1(x) \mid c_2(x) \mid \cdots \mid c_{n-1}(x) \mid$ where $c_i(x) \in F\mathbb{Z}_m$ for all i and $\mid$ denotes concatenation (as in [7, p. 584]). A generating array for C may be formed by concatenating the n circulant matrices that result from taking corresponding cyclic shifts of each m-tuple of the generator: the unreduced generating array $\mathcal{G} = [\mathcal{G}_0\ \mathcal{G}_1 \cdots \mathcal{G}_{n-1}]$ where, for all i, $0 \le i < n$, the j-th row of $\mathcal{G}_i$ is $x^j \cdot c_i(x)$, $0 \le j < m$. Such codes are referred to as row-cyclic.

Alternatively, we may consider the codewords of C to be elements of the group ring $F(\mathbb{Z}_m \times \mathbb{Z}_n)$. Clearly linear code C with generator $\mathcal{G}$ is a vector subspace of $F(\mathbb{Z}_m \times \mathbb{Z}_n)$. We will show that certain of these codes, resulting from careful selection of g, exhibit a stronger structure, that of an ideal in a group ring.

*This work was presented in part at the First International Conference on Finite Fields, Coding Theory, and Advances in Communications and Computing, Las Vegas, Nevada, August, 1991.

1.2. Metacyclic Codes

A metacyclic group is an extension of a cyclic group by a cyclic group. We will denote such a group as $G(m, n, r)$ where

$$G(mn, n, r) = \{x^i y^j : x^m = y^n = 1,\ yx = x^r y\}$$

where $\gcd(m, r) = 1$ and $r^n \equiv 1 \bmod m$. The r parameter may be informally viewed as the measure of *non-abelian-ness* of the group. If $r = 1$, then $G(m, n, r)$ is the abelian $\mathbb{Z}_m \times \mathbb{Z}_n$. We will consider metacyclic groups for which neither m nor n is 1.

If field $F = \mathrm{GF}(p^q)$, group ring $FG(m, n, r)$ consists of polynomials of the form

$$f(x, y) = \sum_{j=0}^{n-1} \sum_{i=0}^{m-1} f_{ij}\, x^i y^j,\ f_{ij} \in F. \tag{1}$$

Define addition in the group ring in the obvious way. Multiplication is performed in the usual polynomial manner, but, like multiplication in the underlying group, may be noncommutative. We will assume thrughout the remainder of this article that $\gcd(p, m) = 1$ ensuring that $F\mathbb{Z}_m$ is semi-simple [3].

An element of $FG(m, n, r)$ may be written as in (1) or alternatively as a sequence of n polynomials in $F\mathbb{Z}_m$:

$$f(x, y) = \mid f_0(x) \mid f_1(x) \mid \cdots \mid f_{n-1}(x) \mid,\ f_i(x) \in F\mathbb{Z}_m. \tag{2}$$

We will reserve the term metacyclic code for ideals in $FG(m, n, r)$ where $G(m, n, r)$ is nonabelian, i.e., where $r \neq 1$.

2. Defining the Codes

2.1. The Associated Cyclic Code

Some quasi-cyclic codes are ideals in $FG(m, n, r)$. Such codes are isomorphic to cyclic codes in $F\mathbb{Z}_m$. To show this, we begin by defining the isomorphic cyclic code.

Let C_i^Q represent a Q-cyclotomic coset (mod m) containing i, i.e., $C_i^Q = \{i, iQ, iQ^2, iQ^3, \ldots\}$ with all elements taken mod m. If $F = \mathrm{GF}(p^q)$, cyclic code $\mathfrak{A} \subset F\mathbb{Z}_m$ has its set of nonzeros $\mathfrak{Z} = \{\omega^i : i \in S\}$ where ω is a primitive m-th root of unity and S is the union of one or more p^q-cyclotomic cosets (mod m). We will use $\mathfrak{A}$ to build a quasi-cyclic code only if the corresponding set S satisfies two conditions: first, $0 \notin S$, i.e., ω^0 is not a nonzero of $\mathfrak{A}$. Additionally, S must be a union of r-cyclotomic cosets (mod m). For each qualifying (m, n, r), at least one such S and consequently one such $\mathfrak{A}$ exists. Let such an $\mathfrak{A}$ have dimension k and idempotent generator $\epsilon(x)$. For a given $FG(m, n, r)$, one or more such codes may be found. We define such a code.

Definition. For a given $FG(m, n, r)$, if cyclic code $\mathcal{C} \in F\mathbb{Z}_m$ satisfies the conditions above, then $\mathcal{C}$ is an associated cyclic code for $FG(m, n, r)$.

The identification of appropriate generators requires the definition of an isomorphism on $F\mathbb{Z}_m$.

Definition. Let isomorphism $\rho : F\mathbb{Z}_m \rightarrow F\mathbb{Z}_m$ where $\rho : f_i x^i \mapsto f_i x^{ir}$ for $f_i \in F$.

Since $\gcd(m, r) = 1$, ρ is an automorphism on the group ring $F\mathbb{Z}_m$. Choose $\mathcal{C} \subset F\mathbb{Z}_m$ as described above with corresponding S, a union of p^q cyclotomic cosets that identifies the nonzeroes of $\mathcal{C}$, also a union of r-cyclotomic cosets. Then $\mathcal{C}$ is stable under ρ, i.e., ρ is an automorphism of $\mathcal{C}$, and $\rho(\epsilon(x)) = \epsilon(x)$ [2]. And since $r^n \equiv 1 \bmod m$, $\rho^n(c(x)) = c(x)$ for any $c(x)$ in $\mathcal{C}$. We define a product of successive images of $c(x)$ under ρ.

Definition. Let $N_\rho(c(x)) = \Pi_{i=0}^{n-1} \rho^i(c(x))$.

Note that if $\mathcal{C}$ is irreducible and ρ generates the Galois group of $\mathcal{C}$ over GF(p), the product above is the norm of the Galois group [5].

2.2. *Code Generators*

Having identified an associated cycle code $\mathcal{C}$, select $c(x) \in \mathcal{C}$ such that $N_\rho(c(x)) = \epsilon(x)$. At least one such element exists, $c(x) = \epsilon(x)$, but, in fact, many such elements may be found. Define a sequence of n elements of $\mathcal{C}$.

Definition. Let $\mathcal{C}$ be an associated cyclic code for $FG(m, n, r)$ with idempotent generator $\epsilon(x)$. A ρ-generator in $FG(m, n, r)$ is of the form

$$g = \mid \epsilon(x) \mid c(x) \mid c(x) \cdot \rho(c(x)) \mid c(x) \cdot \rho(c(x)) \cdot \rho^2(c(x)) \mid \cdots \mid \Pi_{i=0}^{n-2} \rho^i(c(x)) \mid \quad (3)$$

where $c(x) \in \mathcal{C}$ and $N_\rho(c(x)) = \epsilon(x)$.

A ρ-generator (3) may be used to create a generating matrix $\mathcal{G}$ for a row-cyclic code as in 1.1. Such a code will have dimension $k = \dim(\mathcal{C})$ and will be isomorphic (as a vector space) to $\mathcal{C}$.

Note. If $F = \mathrm{GF}(2)$ and $\mathcal{C}$ is minimal, g belongs to a more general family of generators, studied by Piret [9], of the form

$$g = \mid \epsilon(x) \mid c_1(x) \mid c_2(x) \mid \cdots \mid c_{n-1}(x) \mid \quad (4)$$

where for all i, $c_i(x) \in \mathcal{C}$, a minimal (m, k, d) binary cyclic code with idempotent generator $\epsilon(x)$. For every i, $c_i(x) = \epsilon(x) \cdot f(x)^{b(i)}$ where $f(x)$ is a primitive polynomial of degree $m - k$, $b(i)$ an integer-valued function, and $f(x)^{b(i)}$ is taken mod $f(x)$. He showed that, in some cases, such codes rival the best known linear block codes of like length and dimension.

We note that if $r = 1$, only one generator is possible since $\rho = 1$ and $N_\rho(c(x)) = \epsilon(x)$ only if $c(x) = \epsilon(x)$. Then $g = \mid \epsilon(x) \mid \epsilon(x) \mid \cdots \mid \epsilon(x) \mid$ and the codewords generated are simply n-repetitions of a codeword of $\mathcal{A}$. Such a code is an ideal in $F(\mathbb{Z}_m \times \mathbb{Z}_n)$, but, with dimension k and minimum distance equal to n times the minimum distance of $\mathcal{A}$, is uninteresting.

We wish to show that the quasi-cycle code generated by a ρ-generator is an ideal in $FG(m, n, r)$. To do so, we relate ρ to multiplication in $FG(m, n, r)$.

Lemma 1. Let $\rho : F\mathbb{Z}_m \to F\mathbb{Z}_m$, $\rho : f_i x^i \mapsto f_i x^{ir}$. If $d(x, y) = \mid d_0(x) \mid d_1(x) \mid \cdots \mid d_{n-1}(x) \mid \in FG(m, n, r)$, then

$$y \cdot (\mid d_0(x) \mid d_1(x) \mid \cdots \mid d_{n-1}(x) \mid) = \mid \rho(d_{n-1}(x)) \mid \rho(d_0(x)) \mid \cdots \mid \rho(d_{n-2}(x)) \mid .$$

Proof. As an element of $FG(m, n, r)$

$$d(x, y) = d_0(x) + d_1(x) \cdot y + \cdots + d_{n-1}(x) \cdot y^{n-1}.$$

$$y \cdot d(x, y) = y \cdot d_0(x) + y \cdot d_1(x) \cdot y + \cdots + y \cdot d_{n-1}(x) \cdot y^{n-1}.$$

In $G(m, n, r)$, $y \cdot x = x^r \cdot y$. Therefore, $y \cdot x = \rho(x) \cdot y$. By the linearity of ρ

$$y \cdot d(x, y) = \mid \rho(d_{n-1}(x)) \mid \rho(d_0(x)) \mid \cdots \mid \rho(d_{n-2}(x)) \mid . \qquad \square$$

Note. For the remainder of this article, we simplify notation by omitting the use of the indeterminate x in referring to elements of $F\mathbb{Z}_m$, e.g., $c(x)$ will be referred to as c.

In Theorem 1, matrix $\mathcal{G}$ is derived from g as described in 1.1.

Theorem 1. *A quasi-cyclic code $\mathcal{Q}$ generated by $\mathcal{G}$, the generating matrix derived from ρ-generator g is a left ideal in $FG(m, n, r)$ with generator g.*

Proof. Let $\mathcal{C}$ be the left ideal generated by g in $FG(m, n, r)$. Let $\mathcal{Q}$ be the quasi-cyclic code generated by $\mathcal{G}$. The row space of $\mathcal{G}$ includes all elements of the form $x^i \cdot g$. Clearly, $\mathcal{Q} \subseteq \mathcal{C}$.

$$y \cdot g = y \cdot (\mid \epsilon \mid c \mid c \cdot \rho(c) \mid \cdots \mid \prod_{i=0}^{n-2} \rho^i(c) \mid)$$

$$= \mid \prod_{i=1}^{n-1} \rho^i(c) \mid \rho(\epsilon) \mid \rho(c) \mid \cdots \mid \prod_{i=1}^{n-2} \rho^i(c) \mid \text{ by Lemma 1}$$

$$= \mid \prod_{i=1}^{n-1} \rho^i(c) \mid \epsilon \mid \rho(c) \mid \cdots \mid \prod_{i=1}^{n-2} \rho^i(c) \mid \text{ since } \rho(\epsilon) = \epsilon$$

c was chosen so that $\Pi_{i=0}^{n-1} \rho^i(c) = \epsilon$. Let $f = \Pi_{i=1}^{n-1} \rho^i(c) \in \mathcal{A}$. Then $\epsilon = f \cdot c$ and

$$y \cdot g = | f | f \cdot c | f \cdot c \cdot \rho(c) | \cdots | f \cdot \prod_{i=0}^{n-2} \rho^i(c) |$$

$$= f(| \epsilon | c | c \cdot \rho(c) | \cdots | \prod_{i=0}^{n-2} \rho^i(c) |)$$

This element belongs to the row space of $\mathcal{G}$ and hence is in $\mathcal{Q}$. It follows that any element of the form $y^i \cdot g \in \mathcal{Q}$. Since $\mathcal{Q}$ is linear, $\mathcal{C} \subseteq \mathcal{Q}$. □

To simplify notation, we will refer to the quasi-cyclic code generated by g built from c (as above) as $\mathcal{C}(c)$.

Lemma 2. If $F = \mathrm{GF}(p^q)$ and $n \equiv 1 \bmod p$, then ρ-generators in $FG(m, n, r)$ are idempotent.

Proof. Let g be a ρ-generator in $FG(m, n, r)$. Multiplying in $FG(m, n, r)$:

$$g \cdot g = \epsilon \cdot g + c \cdot y \cdot g + c \cdot \rho(c) \cdot y^2 \cdot g + \cdots + \prod_{i=0}^{n-1} \rho^i(c) \cdot y^{n-1} \cdot g.$$

Distributing to each of the n m-tuples in g and using Lemma 1:

$$g \cdot g = (| \epsilon | c | c \cdot \rho(c)) | c \cdot \rho(c) \cdot \rho^2(c) | \cdots | \prod_{i=0}^{n-2} \rho^i(c)) |)$$

$$+ (| c \cdot \prod_{i=1}^{n-1} \rho^i(c) | c | c \cdot \rho(c) | c \cdot \rho(c) \cdot \rho^2(c) | \cdots | \prod_{i=0}^{n-2} \rho^i(c) |)$$

$$+ (| c \cdot \rho(c) \cdot \prod_{i=2}^{n-1} \rho^i(c) | c \cdot \rho(c) \cdot \prod_{i=2}^{n} \rho^i(c) | c \cdot \rho(c) | \cdots | \prod_{i=0}^{n-2} \rho^i(c) |)$$

$$+ \cdots$$

$$+ (| \prod_{i=0}^{n-2} \rho^i(c) \cdot \rho^{n-1}(c) | c | c \cdot \rho(c) | c \cdot \rho(c) \cdot \rho^2(c) | \cdots | \prod_{i=0}^{n-2} \rho^i(c) |)$$

Since c was chosen so that $N_\rho(c) = \Pi_{i=0}^{n-1} \rho^i(c) = \epsilon$, and $n \equiv 1 \bmod (\mathrm{char}\ F)$, adding the n subproducts above yields

$$g \cdot g = | \epsilon | c | c \cdot \rho(c) | c \cdot \rho(c) \cdot \rho^2(c) | \cdots | \prod_{i=0}^{n-2} \rho^i(c) | = g. \qquad \square$$

Example. Consider codes in $\mathbb{F}_2 G(11, 5, 3)$. Let $S = C_1^2 = \{1, 2, \ldots, 10\} = C_1^3 \cup C_2^3$. Let code $\mathcal{A} \subset \mathbb{F}_2 \mathbb{Z}_{11}$ have nonzeros ω^i, where $i \in S$ and ω is a primitive 11-th root of one. Writing elements of $\mathbb{F}_2 \mathbb{Z}_{11}$ as sequences of elements of $\mathbb{F}_2$, $\mathcal{A}$ has idempotent generator $\epsilon = 01111111111$. Let $c = 00100000100$. Then $N_\rho(c) = \epsilon$. The ρ-generator built from c is $g = 01111111111\ 00100000100\ 00011000101\ 10011110010\ 11011001100$. $\mathcal{C}(c)$ is a (55, 10) 20 code and a left ideal in $\mathbb{F}_2 G(11, 5, 3)$.

3. Algebraic Structure

3.1. *The Decomposition of $FG(m, n, r)$*

If $F = \mathrm{GF}(p^q)$ and $\gcd(p, mn) = 1$, $FG(m, n, r)$ is semi-simple [3]. As in the semi-simple abelian case, such group rings (and semi-simple nonabelian group rings in general) decompose to unique direct sums of minimal two-sided ideals [6]. In the non-abelian case, however, one or more of the minimal two-sided ideals always decompose to one-sided ideals in numerous ways [11]. In $FG(m, n, r)$, certain of the minimal two-sided ideals decompose to n minimal left (or right) ideals. The codes described above have been shown to be such minimal one-sided ideals in $FG(m, n, r)$ [10].

Alternate decompositions of decomposable two-sided ideals in $FG(m, n, r)$ can be determined by using absolutely irreducible representations of $G(m, n, r)$ over a splitting field. The idempotent generators of those two-sided ideals can be determined by taking the traces of matrix representations that correspond to the absolutely irreducible representations of degree n. Bases for the multi-dimensional matrix representations can be varied resulting in different decompositions. If $\mathcal{A}$ is minimal in $F\mathbb{Z}^m$, i.e., contains no nontrivial subcodes, we may use a simple, direct method (described below) to generate codes that are isomorphic as vector spaces but may vary in their weight distributions. When $\mathcal{A}$ is minimal and $FG(m, n, r)$ semi-simple, it can be shown that all minimal ideals in $FG(m, n, r)$ which are not two-sided are produced by a ρ-generator [10].

3.2. *When $\mathcal{A}$ Is Minimal*

Assume that $FG(m, n, r)$ is semi-simple, $F = \mathrm{GF}(p^q)$ and associated cyclic code $\mathcal{A} \subset F\mathbb{Z}_m$ is minimal and of dimension k. We begin by observing that left ideals in $FG(m, n, r)$ that are subcodes of the same minimal two-sided ideal have the same associated cyclic code [12]. Varying the choice of c for the ρ-generator will produce different codes. Since $\mathcal{A}$ is minimal, $\mathcal{A}$ is isomorphic to a finite field [7, p. 255]. Let isomorphism $\psi : \mathrm{GF}(p^k) \rightarrow \mathcal{A}$, $\psi : \beta_0 \mapsto \epsilon$ where β is a primitive element of $\mathrm{GF}(p^k)$ and ϵ is the idempotent generator of $\mathcal{A}$. Choose $b \in \mathcal{A}$ such that $<b> = \mathcal{A}^* = \mathcal{A} - 0$. Then ψ is fully described by $\psi : \beta \mapsto b$. Use the arithmetic of $\mathrm{GF}(p^k)$ to write $b^0 = \epsilon$.

Since $\mathcal{A}$ is invariant under ρ, there exists t, such that $\rho(b) = b^t$. Seeking codewords $c \in \mathcal{A}$ to form ρ-generators, then reduces to searching for $c = b^p$ such that

$$N_\rho(c) = \prod_{i=0}^{n-1} \rho^i(c) = \prod_{i=0}^{n-1} \rho^i(b^p) = b^0 = \epsilon.$$

Theorem 2, Hilbert's Satz 90 [4], [5], and a corollary simply the search.

Theorem 2. *Let minimal cyclic code $\mathcal{A} \subset F\mathbb{Z}_m$ have idempotent generator ϵ with automorphism ρ as defined above. $N_\rho(c) = \epsilon$ iff $c = \rho(a) \cdot a^{-1}$ for some $a \in \mathcal{A}$.*

The following corollary tells where such elements c may be found.

Corollary. Let $\mathcal{A}$ be a minimal associated cyclic code for $FG(m, n, r)$ and let b be a cyclic generator of $\mathcal{A}^*$. If $\rho(b) = b^t$, then c may be used to form a ρ-generator iff $c \in \langle b^{t-1} \rangle$.

Proof. By Theorem 2, $c = \rho(a) \cdot a^{-1}$ for some $a \in \mathcal{A}$. Since b generates $\mathcal{A}^*$, $\exists\, p$ such that $a = b^p$. Then $c = (b^p)^t \cdot b^{-p} = (b^{t-1})^p$. □

Given a minimal associated cyclic code, we first locate b, a cyclic generator of $\mathcal{A}^*$, and determine t where $\rho(b) = b^t$. All elements of $\langle b^{t-1} \rangle$ may be used as c to form ρ-generators. For $\mathcal{A}$ of large dimension, there may be a large number of such candidates. But all c do not form inequivalent codes.

Definition. Codes C, $C' \subseteq FG$ are said to be combinatorially equivalent if there exists a bijection $\gamma : G \to G$ which extends to $\gamma : FG \to FG$ such that $\gamma\ (C) = C'$.

Clearly combinatorially equivalent codes have identical weight distributions.

The codewords of $\mathcal{C}(c)$ and $\mathcal{C}(d)$ may be considered to be sequences of field elements. The $\mathcal{C}(d)$ is combinatorially equivalent to $\mathcal{C}(c)$ if every codeword of $\mathcal{C}(d)$ is the permutation of the field elements that constitute a distinct codeword of $\mathcal{C}(c)$. Theorem 3 states a sufficient condition for such a relationship.

Theorem 3. *Let $\mathcal{A} \subset FG(m, n, r)$ with idempotent generator ϵ such that $\rho(\epsilon) = \epsilon$. Let $c, d \in \mathcal{A}$. If $N_\rho(c) = N_\rho(d) = \epsilon$ and $d = x^v \rho^i(c)$ for some positive integers i and v, then codes $\mathcal{C}(c)$ and $\mathcal{C}(d)$ are combinatorially equivalent.*

Proof. Let $\mathcal{C}(c)$ have generator

$$g_1 = \mid \epsilon \mid c_0 \mid c_0 \cdot c_1 \mid c_0 \cdot c_1 \cdot c_2 \mid \cdots \mid \prod_{i=0}^{n-2} c_i \mid$$

where $c_i = \rho^i(c)\ \forall\ i,\ 0 \le i < n$. Without loss of generality, assume that $\mathcal{C}(d)$ has generator

$$g_2 = \mid \epsilon \mid d_0 \mid d_0 \cdot d_1 \mid d_0 \cdot d_1 \cdot d_2 \mid \cdots \mid \prod_{i=0}^{n-2} d_i \mid$$

where $d_i = \rho^i(d)\ \forall\ i,\ 0 \le i < n$, and $d = x^v \rho(c) = x^v \cdot c_1$ for some $v \ge 1$. Since $\rho(x) = x^r$, $d_i = \rho(d_{i-1}) = x^{vr^i} \cdot c_{i+1}$. Therefore,

$$g_2 = \mid \epsilon \mid x^{\mathrm{v}} \cdot c_1 \mid x^v \cdot c_1 \cdot x^{vr} \cdot c_2 \mid \cdots \mid \prod_{i=1}^{n-1} (x^{vr^{i-1}} \cdot c_i) \mid .$$

We define $\gamma : G \rightarrow G$ as $\gamma : x^i y^j \mapsto x^{i+p} y^{j-1}$ where $p = \Sigma_{i=0}^{n-2}\, v \cdot r^i$ for $j = 0$, $p = 0$ for $j = 1$, and $p = \Sigma_{i=0}^{j-2}\, v \cdot r^i$ for $1 < j < n$. γ is a bijective and is extended to $FG(m, n, r)$ in the usual way; γ is weight preserving. We need only show that for any $u \in \mathcal{C}(c)$, $\gamma(u) \in \mathcal{C}(d)$. Let $u \in \mathcal{C}(c)$. Since $\mathcal{A}$ and $\mathcal{C}(c)$ are of equal dimension k, $\exists\ a \in \mathcal{A}$ such that

$$u = a \cdot (\mid \epsilon \mid c_0 \mid c_0 \cdot c_1 \mid \cdots \mid \prod_{i=0}^{n-2} c_i \mid)$$

with a considered an element of $FG(m, n, r)$. Then

$$u = \mid a \mid a \cdot c_0 \mid a \cdot c_0 \cdot c_1 \mid \cdots \mid a \cdot \prod_{i=0}^{n-2} c_i \mid .$$

$$\gamma(u) = \mid a \cdot c_0 \mid x^v \cdot a \cdot c_0 \cdot c_1 \mid x^{v+vr} \cdot a \cdot c_0 \cdot c_1 \cdot c_2 \mid \cdots$$

$$\mid x^{(v+vr+\cdots+vr^{n-2})} \cdot a \cdot \prod_{i=0}^{n-1} c_i) \mid)$$

$$= a \cdot c_0 \, (\mid \epsilon \mid x^v \cdot c_1 \mid x^v \cdot c_1 \cdot x^{vr} \cdot c_2 \mid \cdots \mid \prod_{i=1}^{n-1} (x^{vr^{i-1}} \cdot c_i) \mid)$$

with $a \cdot c_0$ considered an element of $FG(m, n, r)$

$$= a \cdot c_0 \cdot g_2 \in \mathcal{C}(d).$$ □

We may simplify the search for nonequivalent $\mathcal{C}(c)$ by considering cosets of $\mathcal{A}^*$ formed as follows. Let H_0 be the set of all distinct cyclic shifts of ϵ, i.e., $H_0 = \{x^i \cdot \epsilon : 0 \le i < m\}$. H_0 is a multiplicative cyclic subgroup of $\mathcal{A}^*$ [13] with order that can be determined. Let S be the set of exponents of ω (a primitive m-th root of one) that correspond to the nonzeros of $\mathcal{A}$, $S = C_i^{p^q}$ (a cyclotomic coset mod m). Then $|H_0| = m \,/\, \gcd(m, i)$. Partition $\mathcal{A}^*$: $\mathcal{A}^*/H_0 = H_0, H_1, \ldots, H_{h-1}$ where (if b generates $\mathcal{A}^*$ as above) $b^i \in H_i$ and $h = |\mathcal{A}^*| \,/\, |H_0|$. Each coset consists of all cyclic shifts of a codeword of $\mathcal{A}^*$; $H_i = \{x^j b^i\}$.

If $s = \gcd(\,|\mathfrak{A}^*|, t-1)$, $<b^{t-1}> \; = \; <b^s>$ and $|<b^{t-1}>| = |\mathfrak{A}^*| \,/\, s$. If H_i contains elements of $<b^{t-1}>$, it contains exactly w such elements where $w = \gcd(\,|\,<b^{t-1}>|, |H_0|\,)$. If we consider ρ acting on such a coset H_i, $\rho : H_i \to H_{it \bmod h}$ since $\rho(x^j b^i) = x^{jv} b^{it}$. Thus ρ partitions cosets containing elements of $<b^{t-1}>$ into sequences.

To determine the distinct sequences of such cosets consider cyclotomic cosets C_i^t mod p where $p = |<b^{t-1}>|/w$ is the number of cosets with elements in $<b^{t-1}>$. With s as defined above, each distinct C_i^t identifies a distinct coset sequence: $\{H_{sj} : j \in C_i^t\}$. For each C_i^t let $c_i = (b^i)^s$. The set $\{\mathcal{C}(c_i)\}$ consists of all possible nonequivalent codes with the desired structure.

Example. In $\mathbb{F}_2G(11, 5, 3)$ (as in Example in Section 2.2), $\mathfrak{A}$ has dimension 10, $\mathfrak{A} \cong \mathrm{GF}(2^{10})$. $|H_0| = 11$. There are $h = (2^{10} - 1) / 11 = 93$ cosets. $\mathfrak{A}^*$ is generated by $b = 01010001111$; $\rho(b) = b^{256}$. $|<b^{255}>| = |<b^3>| = 341$; $s = 3$. $w = \gcd(341,11) = 11$, and $p = 341/11 = 31$. There are 7 distinct 8-cyclotomic cosets mod 31 ($8 \equiv 256$ mod 31): C_i^8 for $i \in \{0, 1, 3, 5, 7, 11, 15\}$. The following codes result; each has dimension 10. The ρ-sequence of codewords shown is c_0, $c_1 = \rho(c_0)$, $c_2 = \rho(c_1)$, $c_3 = \rho(c_2)$, $c_4 = \rho(c_3)$. With the exception of the first code, exhaustive search has shown that none is equivalent to any abelian code. (*Note:* The weight polynomial, $\Sigma_{i=0}^{mn} A_i z^i$, displays the weight distribution, i.e., there are A_i codewords of weight i.)

ρ-sequence of codewords	Generator g	Weight Polynomial (in z)
1. $\epsilon,\epsilon,\epsilon,\epsilon,\epsilon$	$\lvert\epsilon\lvert\epsilon\lvert\epsilon\lvert\epsilon\lvert\epsilon\rvert$	$1+55z^{10}+330z^{20}+462z^{30}+165z^{40}+11z^{50}$
2. $b^3,b^{768},b^{192},b^{48},b^{12}$	$\lvert\epsilon\lvert b^3\lvert b^{771}\lvert b^{963}\lvert b^{1011}\rvert$	$1+88z^{20}+220z^{24}+440z^{28}+275z^{32}$
3. $b^9,b^{258},b^{576},b^{144},b^{36}$	$\lvert\epsilon\lvert b^9\lvert b^{267}\lvert b^{843}\lvert b^{987}\rvert$	$1+110z^{20}+55z^{24}+275z^{26}+220z^{28}+198z^{30}+110z^{32}+55z^{34}$
4. $b^{15},b^{771},b^{960},b^{240},b^{60}$	$\lvert\epsilon\lvert b^{15}\lvert b^{786}\lvert b^{723}\lvert b^{963}\rvert$	$1+22z^{20}+385z^{24}+330z^{28}+275z^{32}+11z^{40}$
5. $b^{21},b^{261},b^{321},b^{336},b^{84}$	$\lvert\epsilon\lvert b^{21}\lvert b^{282}\lvert b^{603}\lvert b^{939}\rvert$	$1+11z^{10}+55z^{18}+165z^{24}+330z^{28}+462z^{30}$
6. $b^{33},b^{264},b^{66},b^{528},b^{132}$	$\lvert\epsilon\lvert b^{33}\lvert b^{297}\lvert b^{363}\lvert b^{891}\rvert$	$1+66z^{20}+220z^{24}+550z^{28}+165z^{32}+22z^{40}$
7. $b^{45},b^{267},b^{834},b^{720},b^{18}$	$\lvert\epsilon\lvert b^{45}\lvert b^{312}\lvert b^{123}\lvert b^{843}\rvert$	$1+55z^{18}+165z^{24}+165z^{26}+330z^{28}+198z^{30}+110z^{34}$

Example. In $\mathbb{F}_2G(25, 5, 6)$, $\mathfrak{A}$ has dimension 20, $\mathfrak{A} \cong \mathrm{GF}(2^{20})$. $|H_0| = 25$. There are $h = (2^{20} - 1) / 25 = 41943$ cosets. $\mathfrak{A}^*$ is generated by $b = 000001163_8$; $\rho(b) = b^{256}$. $|<b^{255}>| = |<b^{15}>| = 69905$. $w = \gcd(69905, 25) = 5$, and $p = 69905/5 = 13981$.

There are 2797 distinct 256-cyclotomic cosets mod 13981. Of the possible 2797 codes so generated, exhaustive search yielded 162 codes with distinct weight distributions. Minimum weights ranged from 10 to 44.

3.3. Relationship to Abelian Codes

In some cases, a left code in $FG(m, n, r)$ where $r \neq 1$ derived in the manner described above is equivalent to an abelian code. Specifically, g derived from $c = \epsilon$ generates a code that is equivalent to the abelian (mn, k) code that is the n-repetition of $\mathcal{A}$. In most cases, however, codes so generated are no combinatorially equivalent to any abelian code. Conditions under which the codes formed are abelian have yet to be formulated.

4. Conclusion

This article has exhibited the heretofore undetected ideal structure of an attractive class of quasi-cyclic codes. Table 1 displays some quasi-cyclic codes that are ideals in metacyclic group rings. Each has the structure described above or is derived from one or more codes with such a structure. Several of these codes have a minimum distance that equals that of the best known linear code of the same length and dimension.

Table 1. Binary metacyclic codes (in $\mathbb{F}_2 G(M, N, R)$).

<table>
<tr><th>n</th><th>k</th><th>(m, n, r)</th><th>Generator (octal)</th><th>$d_{\min}$</th><th>Best $d_{\min}$ [1]</th></tr>
<tr><td>14</td><td>6</td><td>(7, 2, 6)</td><td>|164|113|</td><td>4</td><td>5</td></tr>
<tr><td>14</td><td>7</td><td>(7, 2, 6)</td><td>previous code augmented</td><td>4</td><td>4</td></tr>
<tr><td>21</td><td>3</td><td>(7, 3, 2)</td><td>|164|164|164|</td><td>12</td><td>12</td></tr>
<tr><td>21</td><td>6</td><td>(7, 3, 2)</td><td>|072|072|047|</td><td>8</td><td>8</td></tr>
<tr><td>27</td><td>6</td><td>(9, 3, 4)</td><td>|356|055|365|</td><td>12</td><td>12</td></tr>
<tr><td>27</td><td>8</td><td>(9, 3, 4)</td><td>|275|456|654|</td><td>10</td><td>12</td></tr>
<tr><td>27</td><td>19</td><td>(9, 3, 4)</td><td>dual of the previous code</td><td>4</td><td>4</td></tr>
<tr><td>55</td><td>10</td><td>(11, 5, 3)</td><td>|0033|2026|1224|0305|0603|</td><td>20</td><td>23</td></tr>
<tr><td>55</td><td>11</td><td>(11, 5, 3)</td><td>previous code augmented</td><td>20</td><td>22</td></tr>
<tr><td>55</td><td>20</td><td>(11, 5, 3)</td><td>|0000|3175|2575|3514|2651|</td><td>16</td><td>16</td></tr>
<tr><td>55</td><td>45</td><td>(11, 5, 3)</td><td>|2350|3027|2730|2334|1744|</td><td>4</td><td>4</td></tr>
<tr><td>63</td><td>3</td><td>(21, 3, 4)</td><td>|3164723|2351647|7235164|</td><td>36</td><td>36</td></tr>
<tr><td>63</td><td>12</td><td>(21, 3, 4)</td><td>|2607663|2143455|3575316|</td><td>24</td><td>24</td></tr>
<tr><td>93</td><td>15</td><td>(31, 3, 5)</td><td>|13410237634|10702646457|17335771337|</td><td>32</td><td>36</td></tr>
<tr><td>93</td><td>16</td><td>(31, 3, 5)</td><td>previous code augmented</td><td>32</td><td>34</td></tr>
<tr><td>93</td><td>77</td><td>(31, 3, 5)</td><td>dual of previous code</td><td>6</td><td>6</td></tr>
<tr><td>110</td><td>10</td><td>(11, 10, 7)</td><td>|1777|0126|0402|2272|1205
3342|0776|3063|0716|1576|</td><td>48</td><td>49</td></tr>
</table>

The well-defined algebraic structure of these codes should allow the formulation of efficient encoding and decoding algorithms and thus increase the practicality of these codes. It is also hoped that the examination of longer length codes of this type will yield new optimal linear codes.

Acknowledgments

The author wishes to thank the referees for their helpful comments and Dr. Shu Lin for his encouragement.

References

1. Brouwer, A.E. and Tom Verhoeff, An Updated Table of Minimum-Distance Bounds for Binary Linear Codes, *IEEE Trans. IT*, Vol. 36, pp. 662-677, (1993).
2. P. Delsarte, Automorphisms of Abelian Codes, *Philips Res. Repts.* Vol. 25, pp. 389-403, (1970).
3. M. Hall, *The Theory of Groups*, Macmillan: New York, NY, (1959).
4. T.W. Hungerford, *Algebra*, Springer-Verlag: New York, NY, (1974).
5. N. Jacobson, *Basic Algebra I*, Freeman: San Francisco, CA, (1974).
6. R. Keown, *An Introduction to Group Representation Theory*, Academic Press: Newark, NJ, (1975).
7. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting codes*, North-Holland: Amsterdam, (1977).
8. W.W. Peterson and E.J. Walden, Jr., *Error-Correcting Codes*, MIT Press: Cambridge, MA, (1972).
9. P. Piret, Good Block Codes Derived from Cyclic Codes, *Electronics Letters*, Vol. 10, pp. 391-392, (1974).
10. R.E. Sabin, Metacyclic Error-Correcting Codes, Ph.D. dissertation, University of Maryland, Baltimore, MD, (1990).
11. R.E. Sabin, On Determining All Codes in Semi-Simple Group Rings, in *Lecture Notes in Comp. Sc., 673, Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer-Verlag: Berlin, pp. 279-290, (1993).
12. R.E. Sabin and S.J. Lomonaco, Metacyclic Error-Correcting Codes, to appear AAECC, 1984.
13. H.J. Zassenhaus, *The Theory of Groups*, Chalice, New York, (1949).