International Journal of Pure and Applied Mathematics
Volume 94 No. 1 2014, 71-80
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v94i1.8

ON THE GENERATORS OF CYCLIC CODES OVER $\mathbb{Z}_m$ OF ANY LENGTH n

Louis Beaugris
Department of Mathematics
C-233, Kean University
1000 Morris Ave, Union, New Jersey, USA

Abstract: Over the last two decades, there have been discoveries of various good codes over the rings $\mathbb{Z}_m$ of integers modulo m. Restrictions have been imposed on the code's alphabet size m and over the code's length n for many reasons. This paper shows a construction of the generators of cyclic codes over $\mathbb{Z}_m$ via the Division Algorithm, with no restrictions on the aforementioned code parameters.

AMS Subject Classification: 94B15
Key Words: cyclic codes, generators, principal ideals, division algorithm

1. Introduction

In the advent of coding theory, codes were constructed over finites fields, especially over $\mathbb{Z}_2$ for computer applications. Although good codes of lenght n have been found over the finite rings of integers modulo m, $\mathbb{Z}_m$, restrictions are usually imposed on the parameters n and m for algebraic reasons [1,2,3,4,5,6,8,10,11,12]. In what follows, we will show a technique for the construction of generators of cyclic codes of lenght n over $\mathbb{Z}_m$, with no restrictions on n and m.

Received: April 2, 2014

We call a set C a code of length n over $\mathbb{Z}_m$ if C is a nonempty subset of $\mathbb{Z}_m^n$. The elements of C are called the codewords and the elements of $\mathbb{Z}_m$ the code alphabet. C is a linear code if it is a $\mathbb{Z}_m$-submodule of $\mathbb{Z}_m^n$. A linear code of length n over $\mathbb{Z}_m$ is cyclic if it is closed under the cyclic shift operation mapping each element $(c_0, c_1, c_2, ..., c_{n-1})$ of C to the element $(c_{n-1}, c_0, c_1, ..., c_{n-2})$. To each codeword c of C we associate a polynomial $c(x)$ via the isomorphism $\mathbb{Z}_m^n \to \mathbb{Z}_m[x]/(x^n - 1)$ mapping $(c_0, c_1, c_2, ..., c_{n-1})$ into $c_0 + c_1x + c_2x^2 + ... + c_{n-1}x^{n-1}$. We call $c(x)$ the polynomial representation of the codeword c and $\mathscr{C}$ the polynomial representation of the code C. The cyclic shift operation in $\mathbb{Z}_m^n$ corresponds to muliplication by x in $\mathbb{Z}_m[x]/(x^n - 1)$. It is easily verified that $\mathscr{C}$ is an ideal of the ring $R_m = \mathbb{Z}_m[x]/(x^n - 1)$ of polynomials.

It should be noted that if $\mathbb{Z}_m$ is a field, then C is a subspace of the vector space $\mathbb{Z}_m^n$. Thus, when n is relatively prme to m and m is prime, the cyclic code $\mathscr{C}$ of length n over $\mathbb{Z}_m$ is associated with principal ideals whose generators are factors of $(x^n - 1)$. When $\mathbb{Z}_m$ is a ring (and not a field) and n is any integer, the ideals in R_m are not necessarily principal. Moreover, we do not have unique factorization, and so there might be several ways of factoring $(x^n - 1)$, which makes it harder to classify the cyclic codes over $\mathbb{Z}_m$. In this paper, we find a technique for the construction of the generators of cyclic codes of length n over $\mathbb{Z}_m$ for any n and m, i.e. the generators of any code with alphabet a set of residue classes.

Before we begin our construction, we say a few words about the Lee distance between two words over $\mathbb{Z}_m$. The Lee weight of an integer i, where $0 \leq i < m$, is defined by $w_L = min\{i, m - i\}$. The Lee weight of a word $c = c_0c_1c_2...c_{n-1}$ is defined by $w_L(c) = \sum_{i=0}^{n-1} w_L(c_i)$. We define the Lee distance between two words u and v by $d_L(u, v) = w_L(u - v)$. [13, p.43]

2. The Construction

We begin with a version of the theorem commonly known as the Ideal Lattice Theorem:

Theorem 2.1. *There is a 1-1 correspondence between the set of ideals of* $\mathbb{Z}[x]/(x^n - 1)$ *and the set of ideals of* $\mathbb{Z}[x]$ *containing* $(x^n - 1)$.

Proof. Let I be an ideal in $\mathbb{Z}[x]$ containing $x^n - 1$. It is easily shown that the set $I^* = \{[f] \in \mathbb{Z}[x]/(x^n - 1) : f \in I\}$ is an ideal in $\mathbb{Z}[x]/(x^n - 1)$ and that the correspondence $\delta : I \to I^*$ is one-to-one. The reader who desires more details should refer to [7, p.233]. □

We find it advantageous to work with the ideals I of $\mathbb{Z}[x]$ containing $x^n - 1$. First, for polynomials $f \in I$, denote by $lc(f)$ the leading coefficient of f. We begin the construction by making the following definitions for nonzero polynomilas in I:

We wish to construct an ideal I with α generators, where α is a positive integer. To that end, we choose a chain of sub-ideals $C_0 \subset C_1 \subset C_2 \subset ...$ of $\mathbb{Z}$. Since Z is Noetherian, this chain must terminate. We choose a chain $C_0 \subset C_1 \subset C_2 \subset ... \subset C_\alpha$.

Let

$$T_\alpha = \{f \in I : lc(f) = 1\},$$

$$C_\alpha = (b_\alpha), \text{ where } b_\alpha = lc(f), \text{ for some } f \in T_\alpha,$$

$$U_\alpha = \{f \in I : lc(f) = b_\alpha\},$$

$$t_\alpha = mindeg(f), \text{ for } f \in U_\alpha,$$

and choose $f_\alpha \in U_\alpha$ such that $deg(f_\alpha) = t_\alpha$.

Now, let

$$T_{\alpha-1} = \{f \in I : deg(f) < t_\alpha\},$$

$$C_{\alpha-1} = (b_{\alpha-1}), \text{ where } b_{\alpha-1} = lc(f), \text{ for some } f \in T_{\alpha-1},$$

$$U_{\alpha-1} = \{f \in I : lc(f) = b_{\alpha-a}\},$$

$$t_{\alpha-1} = mindeg(f), \text{ for } f \in U_{\alpha-1},$$

and choose $f_{\alpha-1} \in U_{\alpha-1}$ such that $deg(f_{\alpha-1}) = t_{\alpha-1}$.

For integers $i > 1$, we recursively define:

$$T_{\alpha-i} = \{f \in I : deg(f) < t_{\alpha-(i-1)}\},$$

$$C_{\alpha-i} = (b_{\alpha-i}), \text{ where } b_{\alpha-i} = lc(f), \text{ for some } f \in T_{\alpha-i},$$

$$U_{\alpha-i} = \{f \in I : lc(f) = b_{\alpha-i}\},$$

$$t_{\alpha-i} = mindeg(f), \text{ for } f \in U_{\alpha-i}.$$

Let $f_{\alpha-i}$ be the choice of a polynomial $U_{\alpha-i}$ of degree $t_{\alpha-i}$.

The following observations are important. T_α is nonempty since I contains $x^n - 1$. Since T_α only has monic polynomials, we see that $T_\alpha = U_\alpha$. Also, by definition of the T_α's, we must have $t_{\alpha-1} < t_\alpha$. Note also that the leading coefficients of the T_α's do form a principal ideal $C_\alpha = (b_\alpha)$. We also have $C_\alpha = \mathbb{Z}$, and $1|b_1|b_2|...|b_\alpha$. Finally, we let $T_0 = U_0 = C_0 = \{0\}$.

We will use the following theorem in constructing the ideals I:

Theorem 2.2. *Let f be a nonzero polynomial in I, and g any nonzero polynomial in $\mathbb{Z}[x]$.*

(I) If f is monic, then there exist unique polynomials q and r in $\mathbb{Z}[x]$ such that $g = qf + r$ and $deg(r) < deg(f)$ or $r = 0$.

(II) If f is not monic with $lc(f) = b$, and g has a leading coefficient $c \neq 0$, where b divides c, then there exist unique polynomials q and r in $\mathbb{Z}[x]$ such that $g = qf + r$ and $deg(r) < deg(g)$, where the leading coefficient of r is not divisible by the leading coefficient of f or $r = 0$.

Proof. (I) The proof of this part can be found in [9, p158].

(II) The proof of this part is similar to the proof of (I). □

We will refer to Part (I) of the previous theorem as the Division Algorithm I (or DAI), and the Part II as the Division Algorithm II (DAII).

Theorem 2.3. *For $\gamma \leq \alpha$, let f_γ be a choice of polynomial in U_γ having minimal degree t_γ. Then, $\{f_\gamma, f_{\gamma-1}, ..., f_2, f_1\}$ forms a set of generators for I. Equivalently,*

$$I =< f_\gamma > + < f_{\gamma-1} > +...+ < f_2 > + < f_1 >.$$

Proof. Let g be any polynomial in I, and let f_γ be a monic polynomial of degree t_γ in U_γ. By DAI, there exist unique polynomials q_γ and r_γ such that $g = q_\gamma f_\gamma + r_\gamma$ and $degr_\gamma < degf_\gamma$ or $r_\gamma = 0$. If $r_\gamma = 0$, then $g \in < f_\gamma >$. So assume $r_\gamma \neq 0$. Note that $r_\gamma \in T_{\gamma-1}$ since $r_\gamma \in I$ and $degr_\gamma < degf_\gamma = t_\gamma$. Thus, r_γ has leading coefficient in $C_{\gamma-1} = (b_{\gamma-1})$. Also, $r_\gamma \notin U_\gamma$ since f_γ is a polynomial of minimal degree in U_γ, and r_γ cannot be monic. Now, pick $f_{\gamma-1}$ of minimal degree $t_{\gamma-1}$ in $U_{\gamma-1}$, thus $lc(f_{\gamma-1}) = b_{\gamma-1}$. By $DAII$, there exist unique polynomials $q_{\gamma-1}$ and $r_{\gamma-1}$ such that $r_\gamma = q_{\gamma-1}f_{\gamma-1} + r_{\gamma-1}$ and $degr_{\gamma-1} < degr_\gamma$ or $r_{\gamma-1} = 0$.

If $r_{\gamma-1} = 0$, then $r_\gamma = q_{\gamma-1}f_{\gamma-1}$ and thus $g = q_\gamma f_\gamma + q_{\gamma-1}f_{\gamma-1}$, i.e. $g \in < f_\gamma > + < f_{\gamma-1} >$. Otherwise, if $r_{\gamma-1} \neq 0$, we substitute r_γ in g and obtain

$$g = q_\gamma f_\gamma + q_{\gamma-1}f_{\gamma-1} + r_{\gamma-1}.$$

For integers $s \leq u - 1$, for $r_s \in T_{s-1}$ and f_{s-1} of minimal degree t_{s-1} in U_{s-1}, there exist unique polynomials q_{s-1} and r_{s-1} such that $r_s = q_{s-1}f_{s-1} + r_{s-1}$, where $degr_{s-1} < degr_s$ or $r_{s-1} = 0$.. Succesive divisions and substitutions yield

$$g = q_\gamma f_\gamma + q_{\gamma-1}f_{\gamma-1} + ... + q_2 f_2 + q_1 f_1 + r_1,$$

where$r_1 \in T_0 = \{0\}$. Therefore,

$$g = q_\gamma f_\gamma + q_{\gamma-1} f_{\gamma-1} + ... + q_2 f_2 + q_1 f_1.$$

Because g is an arbitrary element of I, we have

$$I =< f_\gamma > + < f_{\gamma-1} > + ... + < f_2 > + < f_1 > . \qquad \square$$

The following will be useful:

Theorem 2.4. *Let ψ be a positive integer such that $\psi \leq \alpha$, and let g be a polynomial in I. If $g \in T_\psi$, then $f_1 | \frac{b_1}{b_\psi} g$.*

Proof. Let $g = c_m x^m + c_{m-1} x^{m-1} + ... + c_1 x + c_0$ be a polynomial in T_ψ. Then $lc(g) = c_m = b_\psi d_m$ for some d_m since $c_m \in C = (b_\psi)$, the ideal generated by the leading coefficient of a polynomial in T_ψ.

Consider $g_1 = g - c_m x^m = c_{m-1} x^{m-1} + ... + c_0$ and note that $g_1 \in T_{\psi-1}$ since $degg_1 < degg$. We must also have $c_{m-1} = b_{\psi-1} k = b_\psi k_1 k$ for some integers k_1 and k since $b_\psi | b_{\psi-1}$. Continuing in this fashion, we obtain the expression,

$$g - b_\psi d_m x^m - b_\psi d_{m-1} x^{m-1} - ... - b_\psi d_0 = 0,$$

i.e. $g = b_\psi h$ for some polynomial h. Now, using $DAII$ on $b_1 h$ and f_1, we get $b_1 h = f_1 q + r$, where $r \in T_0 = \{0\}$, and so $b_1 h = f_1 q$, and therefore $f_1 | \frac{b_1}{b_\psi}$. $\square$

In particular, we see that $f_1 | b_1(x^n - 1)$. We also have the following:

Theorem 2.5. *$f_1 = b_1 m(x)$ for some monic polynomial $m(x)$.*

Proof. By the previous theorem we see that f_1 divides $b_1(x^n - 1)$. Thus, there exists a polynomial h of degree $l = n - t_1$ such that $b_1(x^n - 1) = f_1 h$. Let $f_1 = \sum_{i=0}^{t_1} d_i x^i$ and $h(x) = \sum_{j=0}^{l} c_j x^j$, where $d_{t_1} = b_1$. Using the fact that the coefficients of $b_1(x^n - 1)$ are equal to the coefficients of $f_1(x)h(x)$, we have the following equations, (we use s instead of t_1 for better notation)

(0) $d_s c_l = b_1$
(1) $d_s c_{l-1} + d_{s-1} c_l = 0$
(2) $d_s c_{l-2} + d_{s-1} c_{l-1} + d_{s-2} c_l = 0$
$\vdots$
(k) $d_s d_{l-k} + d_{s-1} c_{l-k+1} + d_{s-2} c_{l-2+k} + ... + d_{s-(k-1)} c_{l-1} + d_{s-k} c_l = 0$
$\vdots$
$d_0 c_0 = -b_1.$

From (0), since $d_s = b_1$, we get $c_l = 1$, thus $h(x)$ is monic. Using $c_l = 1$ in (1) we get (1)': $d_{s-1} = -d_s c_{l-1}$, hence $d_s | d_{s-1}$. Using (1)' in (2) we get

$d_s c_{l-2} - d_s(c_{l-1})^2 + d_{s-2} = 0$, or $d_{s-2} = d_s[(c_{l-1})^2 - c_{l-2}]$. Therefore, $d_s | d_{s-2}$. Proceeding inductively on k, if d_s divides $d_{s-1}, d_{s-2}, ..., d_{s-(k-1)}$, i.e. $d_{s-1} = k_1 d_s$, $d_{s-2} = k_2 d_s$, ..., $d_{s-(k-1)} = k_{l-1} d_s$, then we have

$$d_s c_{l-k} + k_1 d_s c_{l-k+1} + k_2 d_s c_{l-k+2} + ... + k_{l-1} d_s c_{l-1} = d_{s-k} c_l,$$

i.e.

$$d_s(c_{l-k} + k_1 c_{l-k+1} + k_2 c_{l-k+2} + ... + k_{l-1} c_{l-1}) = -d_{s-k} c_l.$$

Therefore, by induction, $d_s | d_{s-i}$ for all i. Since d_s divides all the coefficients of f_1, it follows that $f_1 = d_s m(x) = b_1 m(x)$ for some monic polynomial $m(x)$ in $\mathbb{Z}[x]$. □

Although the set $\{f_\alpha, f_{\alpha-1}, ..., f_2, f_1\}$ generates the ideal I, we can find different sets of generators to determine the same ideal I. In the following, we will show that these can be reduced to a unique form. As a result, we can define a particular form for the set of generators so that each ideal in $\mathbb{Z}[x]/(x^n - 1)$ has a unique set of generators of this form.

Theorem 2.6. *Each element f_s, $1 \le s \le \alpha$, in the set $\{f_\alpha, f_{\alpha-1}, ..., f_2, f_1\}$ of generators of the ideal I can be uniquely expressed in the form*

$$f_s = \sum_{i=t_1}^{t_s} a_i x^i + \sum_{j=0}^{t_1-1} c_j x^j,$$

where:

1) $i = t_s \Rightarrow a_i = b_s$,

2) $t_{s-1} \le i \le t_s - 1 \Rightarrow a_i \in \{0, 1, 2, ..., b_{s-1} - 1\}$,

3) $t_{s-2} \le i \le t_{s-1} - 1 \Rightarrow a_i \in \{0, 1, 2, ..., b_{s-2} - 1\}$,

$\vdots$

s) $t_1 \le i \le t_2 - 1 \Rightarrow a_i \in \{0, 1, 2, ..., b_1 - 1\}$, *and* $c_j \in I$.

Proof. In the construction of the set of generators $\{f_\alpha, f_{\alpha-1}, ..., f_2, f_1\}$, many choices were made. Thus, we can find several such sets. Of all these, choose a set $\{f_l, f_{l-1}, f_2, f_1\}$, where l is maximal, and such that all the properties of the theorem hold if $l \ne \alpha$. Therefore, there exists an integer i between t_1 and t_{l-1} such that, for some integer $k < l$, $t_{k-1} \le i \le t_k - 1$ and $a_i \notin \{0, 1, 2, .., b_k - 1\}$. We have $a_i = q b_k + v$ for unique integers q and v, where $0 \le v < b_k$. Assume i is the maximum such value.

Now, we have $f_{l+1} = \sum_{i=t_1}^{t_l+1} a_i x^i + \sum_{j=0}^{t_1-1} c_j x^j$, and $f_k = \sum_{t_1}^{t_k} a'_i x^i + \sum_{j=0}^{t_1-1} c'_j x^j$. We subtract a multiple of f_k from f_{l+1} and obtain,

$$\begin{aligned} g_{l+1} &= a_{t_{l+1}} x^{t_{l+1}} + a_{t_l} x^{t_l} + \cdots + a_{t_k-1} x^{t_k-1} + \cdots + (qb_k + v)x^i \\ &+ \cdots + a_{k-1} x^{t_{k-1}} + \cdots + \sum_{i=j}^{t_1-1} c_j x^j - (qx^{i-t_k}) b_k x^{t_k} + a'_{t_{k-1}} x^{t_{k-1}} + \cdots + \sum_{j=0}^{t_1-1} c'_j x^j) \\ &= a_{t_{l+1}} x^{t_{l+1}} + \cdots + vx^i + \cdots - (qx^{i-t_k})(a' t_{k-1} x^{t_{k-1}} + \cdots), \end{aligned}$$

where $t_{k-1} \leq i \leq t_k - 1$ and $v \in \{0, 1, 2, 3, ..., b_k - 1\}$. Now, replace f_{l+1} by g_{l+1}. Since l and i are maximal, the conditions 1), 2), ..., s) of the theorems must hold for $\{f_l, f_{l-1}, ..., f_2, f_1\}$.

For uniqueness, suppose for integers s such that $1 \leq s \leq l$, there exist polynomials

$$g_s(x) = \sum_{i=t_1}^{t_l} a'_i x^i + \sum_{j=0}^{t_1-1} c'_j x^j$$

in I, where a'_i and c'_i have the same properties as a_i and c_j as stated in the theorem. Consider the polynomial

$$h_s(x) = f_s(x) - g_s(x) = \sum_{j=0}^{t_s} (a_i - a'_i)x^i + \sum_{j=0}^{t_1-1} (c_j - c'_j)x^j$$

Now, assume $f_k = \sum_{i=t_1}^{t_k} a_i x^i + \sum_{j=0}^{t_1-1} c'_j x^j$ is unique for minimal $k \leq s$. Thus, if there exists a polynomial $g_k = \sum_{i=t_1}^{t_k} a'_i x^i + \sum_{j=0}^{t_1-1} c'_j x^j$ with the same properties as f_k as listed in the theorem such that $f_k = g_k$, then, we have

$$\begin{aligned} 0 \neq f_k - g_k &= \sum_{i=t_1}^{t_k} (a_i - a'_i)x^i + \sum_{j=0}^{t_1-1} (c_j - c'_j)x^j \\ &\neq \sum_{i=t_1}^{i<t_k} (a_i - a'_i)x^i + \sum_{j=0}^{t_1-1} (c_j - c'_j)x^j \\ &\neq \sum_{i=t_1}^{t_{k-1}} (a_i - a'_i)x^i + \sum_{j=0}^{t_1-1} (c_j - c'_j)x^j \neq f_{k-1} - g_{k-1}. \end{aligned}$$

We find that $f_{k-1} \neq g_{k-1}$, a contadiction to k being minimal. Therefore, by induction, the polynomials $f_s, f_{s-1}, ..., f_2, f_1$ are unique. □

3. Remarks and Examples

The above construction was performed over $\mathbb{Z}$ instead of $\mathbb{Z}_m$ for two main reasons. First, this helps generalize the construction over any set of inetgers. Second, it is more convenient to prove the theorems over $\mathbb{Z}$ as it is free of zero divisors.

We use our results to contsruct cyclic codes over rings of integers modulo m. The transition is made via the natural reduction map $\mathbb{Z}[x]/(x^n - 1) \to \mathbb{Z}_m/(x^n - 1)$.

We provide an example below for $m = p^k$ as an illustration:
Let C be a cyclic code of length $n = 7$ over $\mathbb{Z}_8$ such that C only contains codewords of even Lee weight. We note that an even-weight word over $\mathbb{Z}_m$ must have an even number of odd entries. Also, it can be quickly verified that a code over $\mathbb{Z}_m$ with only even weight codewords is indeed an ideal of the ring $\mathbb{Z}_m[x]/(x^n - 1)$.

To construct a code C with $\alpha = 3$ generators, we pick a chain $(4) \subset (2) \subset (1)$ of ideals of $\mathbb{Z}_8$, and let
$T_3 = \{f \in C : lc(f) = 1\}$,
$b_3 = 1$,
$t_3 = 5$;

$T_2 = \{f \in C : degf \leq t_3 = 5\}$,
$b_2 = 2$,
$C_2 = (2)$,
$U_2 = \{f \in C : lc(f) = 2\}$,
$t_2 = 3$;

$T_1 = \{f \in C : degf \leq t_2 = 3\}$,
$b_1 = 4$,
$C_1 = (4)$,
$U_1 = \{f \in C : lc(f) = 4\}$,
$t_1 = 0$.

We see that $U_3 = T_3$ and $C_3 = (1) = \mathbb{Z}_8$.

Since $x^7 - 1$ is in C, it can be written as a linear combination of the generators. By the Division Algorithm, we have $x^7 - 1 = f_3 g_3 + r_3$ for unique polynomials g_3 and r_3. Choose $f_3 = x^5 + 2x^4 + 2x^3 + 2x + 5$ as a polynomial of minimal degree in T_3. Then,

$$x^7 - 1 = (x^5 + 2x^4 + 2x^3 + 2x + 5)(x^2 + 6x + 2) + 2x^3 + 7x^2 + 6x + 5,$$

with all operations performed modulo 8. So, we obtain $r_3 = 2x^3 + 7x^2 + 6x + 5$, which is a member of T_2. Now choose $f_2 = 2x^3 + 3x^2 + 6x + 5$ from U_2. then, by the Division Algorithm on r_3 and f_2, we have, $r_3 = f_2 g_2 + r_2$, i.e.,

$$2x^3 + 7x^2 + 6x + 5 = (2x^3 + 3x^2 + 6x + 5).1 + 4x^2,$$

and so $r_2 = 4x^2$. Finally, choosing $f_1 = 4$ in U_1, we have $g_1 = x^2$ and $r_1 = 0$, and we stop. We obtain the expression,

$x^7 - 1 = f_3 g_3 + f_2 g_2 + f_1 g_1 = (x^5 + 2x^4 + 2x^3 + 2x + 5)(x^2 + 6x + 2) + (2x^3 + 5x^2 + 2x + 1) + 4x^2$.

Thus, our technique yields

$$C =< f_3, f_2, f_1 >=< x^5 + 2x^4 + 2x^3 + 2x + 5, 2x^3 + 3x^2 + 6x + 5, 4 >$$

as a code with 3 generators and even-weight codewords.

The above set of generators can be reduced to a unique for $< f_3^*, f_2^*, f_1^* >$, where the coefficients of each f_i^* satisfy the conditions of Theorem 2.5. We find $f_3^* = f_3 + (3x + 3)f_2 + f_1$, $f_2^* = f_2 + (x + 1)f_1$, and $f_1^* = f_1$. It is easily verified that $f_3^* = x^5 + x^3 + 3x^2 + 3x$, $f_2^* = 2x^3 + 3x^2 + 2x + 1$, and of course, $f_1^* = 4$. Indeed, $x^7 - 1$ forms a linear combination of the f_i^*s, as $x^7 - 1 = (x^5 + x^3 + 3x^2 + 3x)(x^2 + 6x + 2) + (2x^3 + 3x^2 + 2x + 1)(5x^3 + 3x^2 + 3) + 4(3x^4 + 5x^2 + 7x + 3)$. We obtain $C^* =< x^5 + x^3 + 3x^2 + 3x, 2x^3 + 3x^2 + 2x + 1, 4 >$ as a cyclic code of lenght $n = 7$ over $\mathbb{Z}_8$ with generators written in a unique form. In this case, C^* is a cyclic code with codewords of even Lee weight.

This paper showed a construction of the generators of cyclic codes over the finite rings $\mathbb{Z}_m$, without imposing restrictions on the size m of the alphabet and the code length n. This construction was realized mainly via the division algorithm, the ascending chain condition on the code C, and choices of the generators. We note that, after constructing these codes, worthwhile coding theory problems that can be considered include finding the parameters such as the code size, its minimum distance, encoding and decoding algorithms.

References

[1] A. Alahmadi, H. Sboui, P. Solé, O. Yemen, Cyclic codes over $M_2(F_2)$, *Journal of the Franklin Institute*, **350** (2013), 2837-2847. DOI: 10.1016/j.jfranklin.2013.06.023

[2] T. Abualrub, Cyclic codes and their duals over $\mathbb{Z}_m$, *Ann Sci Math Quebec*, **23** (1999), 109-118.

[3] M. Al-Ashker, M. Hamoudeh, Cyclic codes over $\mathbb{Z}_2$+u$\mathbb{Z}_2$+$u^2\mathbb{Z}_2$+...+$u^{n-1}\mathbb{Z}_2$, *Turk J of Math*, **35** (2011), 737-749.

[4] T. Blackford, Cyclic codes over $\mathbb{Z}_4$ of oddly even length, *Discrete Applied Mathematics*, **128** (2003), 27-46. DOI: 10.1016/S0166-218X(02)00434-1

[5] I.F. Blake, Codes over certain rings, *IEEE Transactions on Information Theory*, **38** (1972), 1125-1130.

[6] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, *Designs, Codes, and Cryptography*, **6** (1995), 21-35. DOI: 10.1007/BF01390768

[7] D. Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms, 2nd ed.*, Springer, New York (1997).

[8] A.R. Hammons, P. Vijay Kumar, A.R. Calderbank, N.J.A. Sloane, P. Sole, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, *IEEE Transactions on Information Theory*, **40** (1994), 301-319.

[9] T. Hungerford, *Algebra*, Springer, New York (1974).

[10] Y. Jia, S. Lin , C. Xing, On self-dual cyclic codes over finite fields, *IEEE Transactions on Information Theory*, **57** (2011), 2243-2251.

[11] M. Özen, M. Güzeltepe, Cyclic codes over some finite quaternion integer rings, *Journal of the Franklin Institute*, **348** (2011), 1312-1317. DOI: 10.1016/j.jfranklin.2010.02.008

[12] V. Pless, Z. Qian, Cyclic and quadratic residue codes over $\mathbb{Z}_4$, *IEEE Transactions on Information Theory*, **42** (1996), 1594-1600.

[13] J.H. Van Lint, *Introduction to Coding Theory, 2nd ed.*, Springer, Berlin (1999).