Ann. Sci. Math. Québec **23** (1999), no. 2, 109–118.

CYCLIC CODES AND THEIR DUALS OVER $\mathbb{Z}_m$

TAHER ABUALRUB

RÉSUMÉ. Nous étudions dans ce papier les codes cycliques sur Z_m comme étant des Z_m-sous-modules de Z_mG et nous déterminons leurs ensembles générateurs minimaux. Nous étudions aussi les codes duals des codes cycliques et nous déterminons leurs ensembles générateurs en tant qu'idéaux dans Z_mG. Tout au long de ce papier, nous supposons que $m = q^e$, q un nombre premier et $(n, q) = 1$.

ABSTRACT. In this paper we study the cyclic codes over Z_m as being Z_m-submodules of Z_mG and we find their minimal generating sets. We also study the dual codes of cyclic codes and find their generators as being ideals in Z_mG. Throughout this paper, we assume $m = q^e$, q is a prime number and $(n, q) = 1$.

1. Introduction and preliminaries. Linear and cyclic codes over rings have been discussed in a series of papers originating with Blake [3] and Wasson [9]. In recent years, more work has been done for codes over Z_m; it has been shown that some binary nonlinear codes are binary images of appropriate linear codes over Z_4 [6]. We start by listing some important definitions needed for this work.

Definition 1.1. Let $u = (u_1, \ldots, u_n)$ and $v = (v_1, \ldots, v_n)$ be two vectors over Z_m. We define an inner product over Z_m by $u \cdot v = u_1v_1 + \cdots + u_nv_n$. If $u \cdot v = 0$, we say u and v are orthogonal.

Definition 1.2. For a group G, the group ring Z_mG is defined to be the set of all formal sums $\sum_{i=1}^{n} r_ig_i$ where $r_i \in Z_m$ and $g_i \in G$ with addition and multiplication defined by

$$\sum_{i=1}^{n} r_ig_i + \sum_{i=1}^{n} s_ig_i = \sum_{i=1}^{n}(r_i + s_i)g_i,$$

$$\sum_{i=1}^{n} r_ig_i \sum_{j=1}^{n} s_jg_j = \sum_{i=1}^{n}\sum_{j=1}^{n} r_is_jg_ig_j.$$

If $G = \langle g \rangle$ is a cyclic group of order n, then

$$Z_mG \cong Z_m[X]/\langle X^n - 1\rangle = Z_m[x].$$

Reçu le 24 mars 1999 et, sous forme définitive, le 1er octobre 1999.

Elements of Z_mG can thus be written as polynomials in x of degree less than n. These in turn can be written as n-tuples. Thus we have the correspondence

$$\sum_{i=1}^{n} r_i g^i \longrightarrow \sum_{i=1}^{n} r_i x^i \longrightarrow (r_1, \ldots, r_n).$$

Throughout this paper, we will assume that $m = q^e$, q is a prime number and G is cyclic of order n and $(n, q) = 1$.

Definition 1.3. A linear code over Z_m is defined to be a Z_m-submodule of Z_mG.

Definition 1.4. By a cyclic code over Z_m, we mean an ideal I in the group ring Z_mG. The elements of I are called codewords.

Definition 1.5. Let C be a linear code over Z_m. We define the dual of C (which is denoted by $C^{\perp}$) to be the set of all vectors which are orthogonal to all codewords in C. i.e.,

$$C^{\perp} := \{u : u \cdot v = 0, \text{for all } v \in C\}. \tag{1}$$

It is easy to see that if C is a linear code, then $C^{\perp}$ is also a linear code.

Definition 1.6. A ring R is called an arithmetical ring if for any ideals A, B, and C in R we have $A \cap (B + C) = (A \cap B) + (A \cap C)$.

The following result was proved in [1].

Theorem 1.1. *Z_mG is a principal ideal ring. Moreover, any cyclic code (ideal) in Z_mG can be written as*

$$\begin{aligned} I &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_s}h_s, h \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1}h_1 + \cdots + q^{l_s}h_s + h \right\rangle, \end{aligned}$$

where $h_1 \mid h_2 \mid \cdots \mid h_s \mid h \mid x^n - 1$ and $e \geq l_0 > l_1 > \cdots > l_s > 0$.

Proof. See Theorem 3.5 in [1]. □

After this theorem has been proved, two questions came to mind: First, what are the minimal generating sets for such codes as being Z_m-submodules of Z_mG? Second, what are the generators of the duals of such codes and what is the relationship between the generating set of a cyclic code and that of its dual? We answer the first question in Section 2 and the second one in Section 3.

The following corollary is needed in the proof later.

Corollary 1.2. *Z_mG is an arithmetical ring.*

Proof. See Lemma 3.13 in [1]. □

2. Cyclic codes over Z_m. To find the minimal generating sets for such codes as being Z_m-submodules of Z_mG, we first consider some special cases until we prove the main case in Theorem 2.3.

Lemma 2.1. *Let $C = \langle g(x) \rangle$ be a cyclic code over Z_m where $g(x)$ is a factor of $x^n - 1$ over Z_m and* $\deg g(x) = r$. *Then C is a free Z_m-submodule of $Z_m G$ with basis*

$$\beta = \left\{ g(x), xg(x), \ldots, x^{n-r-1} g(x) \right\}. \tag{2}$$

Proof. Let $C = \langle g(x) \rangle$ be a cyclic code over Z_m where $g(x)$ is a factor of $x^n - 1$ over Z_m and $\deg g(x) = r$. Note that since $g(x) \mid (x^n - 1)$ in Z_m, then g_0 and g_r are units in Z_m. First, we show that the elements in β are linearly independent. Suppose that,

$$\alpha_0 g(x) + \alpha_1 x g(x) + \cdots + \alpha_{n-r-1} x^{n-r-1} g(x) = 0, \tag{3}$$

for some $\alpha_0, \ldots, \alpha_{n-r-1}$ in Z_m. Then, by comparing coefficients it follows that the constant coefficient in (3) is equal to 0 i.e., $\alpha_0 g_0 = 0$. Since g_0 is a unit in Z_m, then $\alpha_0 = 0$. So, (3) becomes

$$\alpha_1 x g(x) + \cdots + \alpha_{n-r-1} x^{n-r-1} g(x) = 0. \tag{4}$$

By comparing the coefficients of x in (4), we see that $\alpha_1 = 0$. Similarly, we show that $\alpha_2 = 0, \ldots, \alpha_{n-r-1} = 0$ in that order. Therefore β is linearly independent.

Now we show that β spans C. Let $c(x) \in \langle g(x) \rangle$. Then there exists a polynomial $f(x) \in Z_m G$ such that

$$c(x) = g(x) f(x),$$

where $\deg f(x) \leq n - 1$. If $\deg f(x) \leq n - r - 1$, then $c(x) \in \text{span}(\beta)$. Otherwise, by the division algorithm there exist polynomials $\kappa(x)$, $\rho(x)$ such that

$$f(x) = ((x^n - 1)/g(x))\kappa(x) + \rho(x), \tag{5}$$

where $\deg \rho(x) \leq n - r - 1$. Multiplying (5) by $g(x)$ we obtain

$$g(x) f(x) = g(x) \rho(x).$$

Thus $c(x) \in \text{span}(\beta)$. Therefore β spans C. Hence C is a free Z_m-submodule of $Z_m G$ with basis β. □

Lemma 2.2. *Let $C = \left\langle q^l h(x) \right\rangle$ be a cyclic code over Z_m with* $\deg h(x) = r$, $q^l \neq 0$ *and $h(x) \mid (x^n - 1)$ in Z_m. Then C is a Z_m-submodule of $Z_m G$ with minimal generating set.*

$$\beta = \left\{ q^l h(x), q^l x h(x), \ldots, q^l x^{n-r-1} h(x) \right\}.$$

Proof. Let $C = \left\langle q^l h(x) \right\rangle$ be a cyclic code over Z_m with $\deg h(x) = r$, $q^l \neq 0$ and $h(x) \mid (x^n - 1)$ in Z_m. We want to show that β spans C and is a minimal generating set for C (i.e., none of the elements in β is a linear combination of the others). Let $c(x) \in C = \left\langle q^l h(x) \right\rangle$. Then $c(x) = q^l h(x) \mu(x)$ for some $\mu(x) \in Z_m G$. By Lemma 2.1, we obtain that

$$\mu(x) h(x) = \alpha_0 h(x) + \alpha_1 x h(x) + \cdots + \alpha_{n-r-1} x^{n-r-1} h(x),$$

$$c(x) = \alpha_0 q^l h(x) + \alpha_1 q^l x h(x) + \cdots + \alpha_{n-r-1} q^l x^{n-r-1} h(x),$$

for some $\alpha_0, \ldots, \alpha_{n-r-1} \in Z_m$. Therefore β spans C. Now we show that none of the elements in β is a linear combination of the others over Z_m. Suppose that,

$$\begin{aligned} q^l x^i h(x) = {} & \alpha_0 q^l h(x) + \alpha_1 q^l x h(x) + \cdots + \alpha_{i-1} q^l x^{i-1} h(x) \\ & + \alpha_{i+1} q^l x^{i+1} h(x) + \cdots + \alpha_{n-r-1} q^l x^{n-r-1} h(x). \end{aligned} \tag{6}$$

Since the leading coefficient of h is a unit in Z_m and the largest power on the left-hand side of the equation above is $r + i$, then $\alpha_j q^l = 0$ for all $j = i + 1, \ldots, n - r - 1$. So, the above equation becomes

$$q^l x^i h(x) = \alpha_0 q^l h(x) + \alpha_1 q^l x h(x) + \cdots + \alpha_{i-1} q^l x^{i-1} h(x). \tag{7}$$

But the largest power on the left-hand side of this equation is $r + i$ while the largest power on the right-hand side of the equation is $r + i - 1$, a contradiction. Therefore, β is a minimal generating set for C. □

Theorem 2.3. *Let*

$$\begin{aligned} C &= \left\langle q^{l_0} + q^{l_1} h_1 + \cdots + q^{l_s} h_s + h \right\rangle \\ &= \left\langle q^{l_0}, q^{l_1} h_1, \ldots, q^{l_s} h_s, h \right\rangle \end{aligned}$$

be any cyclic code over Z_m, where $h_1 \mid h_2 \mid \cdots \mid h_s \mid h \mid x^n - 1$, $\deg h_i = r_i$, $\deg h = r$ for $i = 1, \ldots, s$ and $e \geq l_0 > \cdots > l_s > 0$. Then C is a Z_m-submodule of $Z_m G$ with minimal generating set given by all the nonzero elements of:

$$\beta = \left\{ \begin{array}{l} h, xh, \ldots, x^{n-r-1}h; q^{l_s}h_s, xq^{l_s}h_s, \ldots, x^{r-r_s-1}q^{l_s}h_s; q^{l_{s-1}}h_{s-1}, \\ xq^{l_{s-1}}h_{s-1}, \ldots, x^{r_s-r_{s-1}-1}q^{l_{s-1}}h_{s-1}; \ldots; q^{l_0}, xq^{l_0}, \ldots, x^{r_1-1}q^{l_0} \end{array} \right\}$$

Proof. Let

$$\begin{aligned} C &= \left\langle q^{l_0} + q^{l_1} h_1 + \cdots + q^{l_s} h_s + h \right\rangle \\ &= \left\langle q^{l_0}, q^{l_1} h_1, \ldots, q^{l_s} h_s, h \right\rangle \end{aligned}$$

be any cyclic code over Z_m, where $h_1 \mid h_2 \mid \cdots \mid h_s \mid h \mid x^n - 1$, $\deg h_i = r_i$, $\deg h = r$ for $i = 1, \ldots, s$ and $e \geq l_0 > \cdots > l_s > 0$. If any of the generators in C above is equal to 0, then we eliminate it from C. So we may assume all the generators above are nonzero. First, we show that β spans C. By Lemma 2.2, it suffices to show that β spans

$$B = \left\{ \begin{array}{c} x^{r-r_s} q^{l_s} h_s, \ldots, x^{n-r_s-1} q^{l_s} h_s; x^{r_s-r_{s-1}} q^{l_{s-1}} h_{s-1}, \ldots, \\ x^{n-r_{s-1}-1} q^{l_{s-1}} h_{s-1}; \ldots, q^{l_0} x^{r_1} \ldots, q^{l_0} x^{n-1} \end{array} \right\}$$

By similarity, we only need to show that β spans $x^{r-r_s} q^{l_s} h_s$. Since $x^{r-r_s} q^{l_s} h_s, q^{l_s} h \in \left\langle q^{l_s} h_s \right\rangle$, by Lemma 2.2, it follows that

$$\begin{aligned} x^{r-r_s} q^{l_s} h_s - q^{l_s} h = {} & \alpha_0 q^{l_s} h_s + \alpha_1 x q^{l_s} h_s + \cdots + \alpha_{r-r_s-1} x^{r-r_s-1} q^{l_s} h_s \\ & + \alpha_{r-r_s} x^{r-r_s} q^{l_s} h_s + \cdots + \alpha_{n-r_s-1} x^{n-r_s-1} q^{l_s} h_s. \end{aligned}$$

Since we may assume that h and h_s are monic, then the largest power on the left-hand side of the above equation is less than r. Therefore, $\alpha_i q^i = 0$ for $i = r - r_s, \ldots, n - r_s - 1$. Hence,

$$x^{r-r_s} q^{l_s} h_s = q^{l_s} h + \alpha_0 q^{l_s} h_s + \alpha_1 x q^{l_s} h_s + \cdots + \alpha_{r-r_s-1} x^{r-r_s-1} q^{l_s} h_s.$$

Hence, β spans B. Now, we show that none of the elements in β is a linear combination of the others. Suppose that $xq^{l_s}h_s$ is a linear combination of some elements in $\beta - \{xq^{l_s}h_s\}$. (Note that the proof works if we choose any other element.) The largest power in $xq^{l_s}h_s$ is equal to $r_s + 1$. By the way we constructed β, it is easy to see that no linear combination of the elements in $\beta - \{xq^{l_s}h_s\}$ will give a polynomial of degree equal to $r_s + 1$. So, β is a minimal generating set for C. □

3. The Dual Of Cyclic Codes Over Z_m. In this section we find the generators of the dual codes and the relationship between the generating set of a code and that of its dual. We start by considering special cases until we prove our main result in Theorem 3.5.

Lemma 3.1. *Let $C = \langle g(x) \rangle$ be a cyclic code over Z_m with $\deg g(x) = r$ and $g(x)|(x^n - 1)$ in Z_m. Then the dual $C^\perp$ of C is given by $C^\perp = \langle k^*(x) \rangle$, where $k(x) = (x^n - 1)/g(x) = k_0 + k_1 x + \cdots + k_{n-r} x^{n-r}$ and $k^*(x) = x^{n-r} k(1/x)$. Moreover, $C^\perp$ is a free Z_m-submodule of $Z_m G$ with basis*

$$\{k^*(x), xk^*(x), \ldots, x^{r-1}k^*(x)\},$$

and rank r.

Proof. The proof follows from Lemma 2.1 and the fact that $(g_0, \ldots, g_r, 0, \ldots, 0)$ is orthogonal to $(k_{n-r}, \ldots, k_0, 0, \ldots, 0)$ and all of its cyclic shifts. □

Lemma 3.2. *Let $C = \langle q^l g(x) \rangle$ be a cyclic code over Z_m with $\deg g(x) = r$ and $g(x)|(x^n - 1)$ in Z_m. Then $C^\perp = \langle q^{e-l}, k^*(x) \rangle$, where $k^*(x)$ is as above.*

Proof. Let $C = \langle q^l g(x) \rangle$ be a cyclic code over Z_m with $\deg g(x) = r$ and $g(x)|(x^n - 1)$ in Z_m. Let $k(x) = (x^n - 1)/g(x) = k_0 + k_1 x + \cdots + k_{n-r} x^{n-r}$, and $k^*(x) = x^{n-r} k(1/x) = k_{n-r} + k_{n-r-1} x + \cdots + k_0 x^{n-r}$. Since $C \subseteq \langle q^l \rangle$ and $C \subseteq \langle g(x) \rangle$, then it follows from Lemma 3.1 that

$$\langle k^*(x) \rangle = \langle g(x) \rangle^\perp \subseteq C^\perp, \text{ and}$$
$$\left\langle q^{e-l} \right\rangle = \left\langle q^l \right\rangle^\perp \subseteq C^\perp.$$

So

$$\left\langle q^{e-l}, k^*(x) \right\rangle \subseteq C^\perp.$$

The other inequality follows from the fact that $(k_{n-r}, \ldots, k_0)$ is orthogonal to $(q^l g_0, \ldots, q^l g_r, 0, \ldots, 0)$ and all of its cyclic shifts. □

Lemma 3.3. *Let C_1, C_2 be two linear codes in Z_{q^e}. Then*

$$(C_1 + C_2)^\perp = C_1^\perp \cap C_2^\perp.$$

Proof. The proof follows from Definition 1.5. □

Before we prove our next result, we need the following definition.

Definition 3.1. Let R be a commutative ring with unity, and let a and b be nonzero elements in R. A least common multiple of a and b is an element r of R such that

i) $a|r$ and $b|r$, and
ii) if $a|c$ and $b|c$, then $r|c$.

Let $A_1 = \langle a_1 \rangle$ and $A_2 = \langle a_2 \rangle$ be two principal ideals in a principal ideal ring. Then it is easy to see that $A_1 \cap A_2$ is a principal ideal generated by one of the least common multiples of a and b.

In case $R = Z_m G$, then it is easy to see that for every monic polynomial $\alpha(x) \in Z_m G$, $[q^i, q^j \alpha(x)] = q^{\max(i,j)} \alpha(x)$. This will be freely used later on.

Theorem 3.4. *Let*

$$\begin{aligned} C &= \left\langle q^{l_0}, q^{l_1} h_1, \ldots, q^{l_s} h_s, h \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1} h_1 + \cdots + q^{l_s} h_s + h \right\rangle, \end{aligned}$$

where $h_1 \mid h_2 \mid \cdots \mid h_s \mid h | x^n - 1$ *and* $e \geq l_0 > l_1 > \cdots > l_s > 0$. *Then*

$$\begin{aligned} C^\perp &= \left\langle q^{e-l_s} k^*, q^{e-l_{s-1}} k_s^*, q^{e-l_{s-2}} k_{s-1}^*, \ldots, q^{e-l_0} k_1^* \right\rangle \\ &= \left\langle q^{e-l_s} k^* + q^{e-l_{s-1}} k_s^* + q^{e-l_{s-2}} k_{s-1}^* + \cdots + q^{e-l_0} k_1^* \right\rangle, \end{aligned}$$

where k_i^* *and* k^* *are defined as in Lemma 3.1.*

Proof. Let

$$\begin{aligned} C &= \left\langle q^{l_0}, q^{l_1} h_1, \ldots, q^{l_s} h_s, h \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1} h_1 + \cdots + q^{l_s} h_s + h \right\rangle, \end{aligned}$$

where $h_1 \mid h_2 \mid \cdots \mid h_s \mid h | x^n - 1$ and $e \geq l_0 > l_1 > \cdots > l_s > 0$. First, we prove the result when $h = 0$. The proof is by induction on s.

If $s = 0$, then $C^\perp = \left\langle q^{l_0} \right\rangle^\perp = \left\langle q^{e-l_0} \right\rangle$.

If $s = 1$, then since $Z_m G$ is an arithmetical ring, by Definition 1.6, Lemma 3.2 and Lemma 3.3, it follows that

$$\begin{aligned} C^\perp &= \left\langle q^{l_0} + q^{l_1} h_1 \right\rangle^\perp \\ &= \left(\left\langle q^{l_0} \right\rangle + \left\langle q^{l_1} h_1 \right\rangle \right)^\perp \\ &= \left\langle q^{l_0} \right\rangle^\perp \cap \left\langle q^{l_1} h_1 \right\rangle^\perp \\ &= \left\langle q^{e-l_0} \right\rangle \cap \left\langle q^{e-l_1}, k_1^* \right\rangle \\ &= \left(\left\langle q^{e-l_0} \right\rangle \cap \left\langle q^{e-l_1} \right\rangle \right) + \left(\left\langle q^{e-l_0} \right\rangle \cap \langle k_1^* \rangle \right) \\ &= \left\langle q^{e-l_1} \right\rangle + \left\langle q^{e-l_0} k_1^* \right\rangle \\ &= \left\langle q^{e-l_1}, q^{e-l_0} k_1^* \right\rangle. \end{aligned}$$

Now, suppose that the theorem holds for $i < s$. Let

$$\begin{aligned} C &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_{s-1}}h_{s-1}, q^{l_s}h_s \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1}h_1 + \cdots + q^{l_{s-1}}h_{s-1} + q^{l_s}h_s \right\rangle. \end{aligned}$$

Then

$$C = \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_{s-1}}h_{s-1} \right\rangle + \left\langle q^{l_s}h_s \right\rangle,$$

and hence by the induction hypothesis, Definition 1.6, Lemma 3.2 and Lemma 3.3, it follows that

$$\begin{aligned} C^{\perp} &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_{s-1}}h_{s-1} \right\rangle^{\perp} \cap \left\langle q^{l_s}h_s \right\rangle^{\perp} \\ &= \left\langle q^{e-l_{s-1}}, q^{e-l_{s-2}}k_{s-1}^*, q^{e-l_{s-3}}k_{s-2}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \cap \left\langle q^{e-l_s}, k_s^* \right\rangle \\ &= \left\langle q^{e-l_{s-1}}, q^{e-l_{s-2}}k_{s-1}^*, q^{e-l_{s-3}}k_{s-2}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \cap \left(\left\langle q^{e-l_s} \right\rangle + \langle k_s^* \rangle \right) \\ &= \left\langle q^{e-l_s}, q^{e-l_s}k_{s-1}^*, \ldots, q^{e-l_s}k_1^*, q^{e-l_{s-1}}k_s^*, q^{e-l_{s-2}}k_{s-1}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \\ &= \left\langle q^{e-l_s}, q^{e-l_{s-1}}k_s^*, q^{e-l_{s-2}}k_{s-1}^*, \ldots, q^{e-l_0}k_1^* \right\rangle. \end{aligned}$$

So, by mathematical induction the theorem holds when $h = 0$. Now, suppose $h \neq 0$, i.e.,

$$\begin{aligned} C &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_s}h_s, h \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1}h_1 + \cdots + q^{l_s}h_s + h \right\rangle. \end{aligned}$$

Then

$$\begin{aligned} C^{\perp} &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_s}h_s, h \right\rangle^{\perp} \\ &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_s}h_s \right\rangle^{\perp} \cap \langle h \rangle^{\perp} \\ &= \left\langle q^{e-l_s}, q^{e-l_{s-1}}k_s^*, q^{e-l_{s-2}}k_{s-1}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \cap \langle k^* \rangle \\ &= \left\langle q^{e-l_s}k^*, q^{e-l_{s-1}}k_s^*, q^{e-l_{s-2}}k_{s-1}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \\ &= \left\langle q^{e-l_s}k^* + q^{e-l_{s-1}}k_s^* + q^{e-l_{s-2}}k_{s-1}^* + \cdots + q^{e-l_0}k_1^* \right\rangle. \end{aligned}$$

The last equation above follows from Theorem 1.1. □

The following corollary follows from Theorem 2.3 and Theorem 3.4.

Corollary 3.5. *Let*

$$\begin{aligned} C &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_s}h_s, h \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1}h_1 + \cdots + q^{l_s}h_s + h \right\rangle, \end{aligned}$$

where $h_1 \mid h_2 \mid \cdots \mid h_s \mid h | x^n - 1$ *and* $e \geq l_0 > l_1 > \cdots > l_s \geq 0$. *Then*

$$\begin{aligned} C^{\perp} &= \left\langle q^{e-l_s}k^*, q^{e-l_{s-1}}k_s^*, q^{e-l_{s-2}}k_{s-1}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \\ &= \left\langle q^{e-l_s}k^* + q^{e-l_{s-1}}k_s^* + q^{e-l_{s-2}}k_{s-1}^* + \cdots + q^{e-l_0}k_1^* \right\rangle, \end{aligned}$$

where k_i^* *and* k^* *are defined as in Lemma 3.1. Moreover,* C *and* $C^{\perp}$ *are* Z_m*-submodules of* Z_mG *with minimal generating sets given by all the nonzero elements of:*

$$\beta = \left\{ \begin{array}{l} h, xh, \ldots, x^{n-r-1}h; q^{l_s}h_s, xq^{l_s}h_s, \ldots, x^{r-r_s-1}q^{l_s}h_s; q^{l_{s-1}}h_{s-1}, \\ xq^{l_{s-1}}h_{s-1}, \ldots, x^{r_s-r_{s-1}-1}q^{l_{s-1}}h_{s-1}; \ldots; q^{l_0}, xq^{l_0}, \ldots, x^{r_1-1}q^{l_0} \end{array} \right\}$$

and

$$\gamma = \left\{ \begin{array}{l} q^{e-l_o}k_1^*, xq^{e-l_0}k_1^*, \ldots; x^{n-t_1-1}q^{e-l_0}k_1^*, q^{e-l_1}k_2^*, xq^{e-l_1}k_2^*, \\ \ldots, x^{t_1-t_2-1}q^{e-t_1}k_2; \ldots; q^{e-l_s}k^*, xq^{e-l_s}k^*, x^{t_{s-1}}q^{e-l_s}k^* \end{array} \right\},$$

where $\deg k_i^* = t_i$, $\deg k^* = t$ *for* $i = 1, \ldots, s$.

Example. Consider the cyclic code $C = \langle x - 1 \rangle$ in

$$Z_4G \cong Z_4[x] / \left\langle x^3 - 1 \right\rangle,$$

where G is a cyclic group of order 3. By Lemma 2.1, C is a free Z_4-submodule of Z_4G with basis $\beta = \{x - 1, x(x - 1)\}$ and rank $(C) = 2$. Moreover, C consists of the 16 codewords

$$\left\{ \begin{array}{c} 0, x-1, 2x+2, 1-x, x^2-x, 2x^2+2x, \\ -x^2+x, x^2-1, 2x^2-x-1, -x^2+2x-1, \\ x^2+x+2, 2x^2+2, x^2+2x+1, 2x^2+x+1, \\ -x^2+1, -x^2-x+2 \end{array} \right\}$$

Thus,

$$C = \left\{ \begin{array}{cccc} 000, & 310, & 220, & 130, \\ 031, & 022, & 013, & 301 \\ 332, & 323, & 211, & 202, \\ 121, & 112, & 103, & 233 \end{array} \right\},$$

and $d(C) = 2$ where $d(C)$ denotes the Hamming weight of C. Also, $C^{\perp} = \left\langle x^2 + x + 1 \right\rangle$ is a free Z_4-submodule of Z_4G with basis $\gamma = \left\{ x^2 + x + 1 \right\}$ and rank$(C^{\perp}) = 1$. Moreover $C^{\perp}$ contains the codewords

$$\left\{ 0, x^2 + x + 1, 2x^2 + 2x + 2, \text{-}x^2 - x - 1 \right\}.$$

Thus,

$$C^{\perp} = \{000, 111, 222, 333\}.$$

Acknowledgment. This paper is a portion of a Ph.D. thesis written by the author under the supervision of Professor Robert Oehmke at University of Iowa. The author wishes to thank Professor Robert Oehmke for his support and his unlimited help during the preparation of this paper. Also the author would like to thank Professors Ibrahim Sadek, Hichem Ben-El-Mechaiekh and Mowaffaq Hajja for remarks that improved the presentation of the paper.

Résumé substantiel en français. Nous étudions dans ce travail les codes cycliques et leurs duaux sur Z_m. Il a été prouvé dans le théorème 2 de [2] que tout code cyclique C est un idéal principal dans l'anneau de groupe Z_mG (où $m = q^e$, q est un nombre premier, G est un groupe abélien d'ordre n et $(n, q) = 1$) et peut être représenté sous la forme:

$$\begin{aligned} C &= \left\langle q^{l_0}, q^{l_1}h_1, \ldots, q^{l_s}h_s, h \right\rangle \\ &= \left\langle q^{l_0} + q^{l_1}h_1 + \cdots + q^{l_s}h_s + h \right\rangle, \end{aligned}$$

où $h_1 \mid h_2 \mid \cdots \mid h_s \mid h | x^n - 1$, et $e \geq l_0 \geq l_1 \geq \cdots \geq l_s$.

Dans la section 2, nous étudions les codes cycliques comme étant des Z_m-sous-modules de Z_mG. Dans le théorème 2.3, nous montrons qu'un ensemble générateur minimal pour de tels codes est de la forme:

$$\beta = \left\{ \begin{array}{l} h, xh, \ldots, x^{n-r-1}h; q^{l_s}h_s, xq^{l_s}h_s, \ldots, x^{r-r_s-1}q^{l_s}h_s; q^{l_{s-1}}h_{s-1}, \\ xq^{l_{s-1}}h_{s-1}, \ldots, x^{r_s-r_{s-1}-1}q^{l_{s-1}}h_{s-1}; \ldots; q^{l_0}, xq^{l_0}, \ldots, x^{r_1-1}q^{l_0} \end{array} \right\}$$

Dans la section 3, nous étudions le dual d'un code cyclique sur Z_m. Dans le théorème 3.5, nous montrons qu'en tant qu'idéal dans l'anneau de groupe Z_mG, le dual $(C^\perp)$ d'un code cyclique quelconque C est engendré par:

$$\begin{aligned} C^\perp &= \left\langle q^{e-l_s}k^*, q^{e-l_{s-1}}k_s^*, q^{e-l_{s-2}}k_{s-1}^*, \ldots, q^{e-l_0}k_1^* \right\rangle \\ &= \left\langle q^{e-l_s}k^* + q^{e-l_{s-1}}k_s^* + q^{e-l_{s-2}}k_{s-1}^* + \cdots + q^{e-l_0}k_1^* \right\rangle, \end{aligned}$$

où $k(x) = (x^n - 1)/h(x)$, $k_i(x) = (x^n - 1)/h_i(x)$, $k^*(x) = k(1/x)$, $k_i^*(x) = k(1/x)$, $i = 1, \ldots, s$, et $h(x)$, $h_i(x)$ sont comme ci-dessus. Pour finir, nous montrons dans le corollaire 3.6 que le dual $(C^\perp)$ de tout code cyclique C pris comme un Z_m-sous-module de Z_mG est engendré par:

$$\gamma = \left\{ \begin{array}{c} q^{e-l_o}k_1^*, xq^{e-l_0}k_1^*, \ldots, x^{n-t_1-1}q^{e-l_0}k_1^*; q^{e-l_1}k_2^*, xq^{e-l_1}k_2^*, \ldots, \\ x^{t_1-t_2-1}q^{e-t_1}k_2; \ldots; q^{e-l_s}k^*, xq^{e-l_s}k^*, x^{t_{s-1}}q^{e-l_s}k^* \end{array} \right\}.$$

REFERENCES

1. T. Abualrub, *Cyclic Codes over the Ring of Integers mod m*, Ph.D. Thesis, University of Iowa, May 1998.
2. T. Abualrub, *Codes over Z_m*, Korean J. Comput. Appl. Math **5** (1998), 99–109.
3. I. F. Blake, *Codes over certain rings*, Information and Control **20** (1972), 396–404.
4. I. F. Blake and R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, New York-London, 1975.
5. R. Gilmer, *Commutative semigroup rings*, Lectures in Mathematics, University of Chicago Press, Chicago, 1984.
6. A. R. Hammons, P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé, *The Z_4-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory **40** (1994), 301–319.
7. G. Karpilovsky, *Commutative Group Algebras*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 78, Marcel Dekker Inc., New York, June 1983.

8. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Mathematical Library, vol. 16, North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.
9. S. K. Wasan, *On Codes over Z_m*, IEEE Trans. Inform. Theory **28** (1982), 117–120.

T. ABUALRUB
AMERICAN UNIVERSITY OF SHARJAH
P.O. BOX 26666
SHARJAH, U.A.E.
E-MAIL ADDRESS: abualrub@aus.ac.ae