Int. J. Open Problems Compt. Math., Vol. 4, No. 2, June 2011
ISSN 1998-6262;
www.i-csrs.org

Codes Over Rings

Mohammed Sabiri[1]

Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès-Saiss
Département de Mathématiques,
BP. 2202 Route d'Imouzzar Fès; Maroc
e-mail: moh_sabiri@yahoo.fr

Abstract

S.D. Berman gave in 1967 a formula of the minimal distance of the FG-codes $(RadFG)^i$ ***for*** $i = 0,\ldots,p^m-1$***, where G is a cyclic group of order*** p^m***, and F a finite field with characteristic*** p***. Our purpose in the present paper is to study codes over finite rings using Berman's ideas. More precisely, we prove that if the code is free over an artinian local ring with finite residue field, then the code has the propriety of the singleton bound and its dimension is exactly that of its coordinatewise projection. Furthermore, a formula for the code distance of free cyclic codes over artinian local rings is established.***

Keywords: *cyclic codes, minimal distance, artinian local ring, coordinatewise projection.*

1 Introduction

A code $\mathcal{C}$ of length n over a finite field F is a subset of the vector space F^n. If $\mathcal{C}$ is a subspace, we say that $\mathcal{C}$ is a linear code and its dimension k is its dimension as a F-vector space. Elements of C are called codewords. The Hamming distance $d(x, y)$ on F^n is given by

$$d(x, y) = \mid \{i : x_i \neq y_i\} \mid$$

[1]Recherche supported by Hassan II Academy as a part of a project in Applied Mathematics and Cryptog.

The Hamming weight of a vector x in F^n is defined as d(x, 0). The minimum (Hamming) distance d of $\mathcal{C}$ is

$$d = d(\mathcal{C}) = min\{d(x, y) : x \neq y \in \mathcal{C}\}$$

For linear codes, this is equivalent to the minimum Hamming weight of the nonzero codewords of $\mathcal{C}$.
A linear code $\mathcal{C}$ is said to be with parameters $[n, k, d]$, if $\mathcal{C}$ is of length n, dimension k and minimum distance d.
A linear code $\mathcal{C}$ of length n is cyclic if any cyclic shift of a codeword of $\mathcal{C}$ is a codeword of $\mathcal{C}$, i.e., if $(c_o, c_1, ..., c_{n-1}) \in \mathcal{C}$ then $(c_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$.
Let G be a finite group and F an arbitrary field. The group algebra FG of the group G over the field F is defined as the algebra over the field F consisting of all possible linear combinations $\sum_{g \in G} k_g g$ of the elements of the group G with the coefficients $k_g \in F$.
It is well known that a code of length n is cyclic if and only if it is an ideal of the ring $A = \frac{F[X]}{(X^n-1)}$. As the algebra A is isomorphic to the group algebra FG where $G =< a >$ is a cyclic group of order n, then cyclic codes may also be considered as the ideals of the group algebra FG. Moreover, if $G =< g \mid g^{p^m} = 1 >$ is a cyclic group of order p^m, then the nontrivial ideals of the group algebra FG are exhausted by the principal ideals $R^j = ((g-1)^j)(j = 1, ..., p^m - 1)$.
One of the serious problems in error correcting codes is the calculation of the minimal distance of linear codes over finite fields. Indeed, a code with minimum distance d can correct $\frac{1}{2}(d-1)$ errors. More generally, the minimum distance of linear codes over finite rings is the attention of authors who have studied these codes. Several authors have studied relation between codes over artinian local rings and its coordinatewise projection. To be more specific, in [2] Walker proved that the minimum distance of a free linear code over an artinian local ring with finite residue field is the same as of its coordinatewise projection.

Motivating by the ideas of Walker, we succeeded in establishing an exact formula for the minimum distance of free cyclic codes of length p^n, where p is the characteristic of the residue field. Further, some basic properties of free codes over an artinian local ring with finite residue field are also obtained.

2 Distance of cyclic codes over finite fields

We begin with Berman's theorem which gives the minimal distance of the powers J^i where J is the (jacobson) radical of the group algebra FG. This theorem is essential in developing the proof of our main result.

Theorem 2.1 ([1], Theorem 1.1)
Let $G =< g \mid g^{p^m} = 1 >$ be a cyclic group of order p^m, F be a field of characteristic $p > 0$, and $I = ((g-1)^i)$ be an ideal of the algebra FG $(1 \leq i \leq p^m - 1)$. We consider the p-expansion of the number i:

$$i = \alpha_1 p^{m-1} + ... + \alpha_m, \qquad (0 \leq \alpha_1, ..., \alpha_m < p).$$

If $\alpha_1 = ... = \alpha_m = p-1$, then $I = (1 + g + ... + g^{p^m-1})$ is one dimensional ideal of the algebra FG and $d(I) = p^m$. Let us assume that for at least one j $(1 \leq j \leq m)$ we have $\alpha_j \neq p-1$, and let α_r be the first of coefficients α_j satisfying this condition. Then

$$d(I) = \begin{cases} p^{r-1}(\alpha_r + 2), \text{ when } (\alpha_{r+1}, ..., \alpha_m) \neq (0, ..., 0), \\ p^{r-1}(\alpha_r + 1), \text{ when } (\alpha_{r+1}, ..., \alpha_m) = (0, ..., 0). \end{cases}$$

We need the next proposition in [4].

Proposition 2.2 *Let $G =< g \mid g^{p^m} = 1 >$ be a cyclic group of order p^m. Then, for all $x \in \{0, ..., p^m - 1\}$ and $a \in (1-g)^x FG = (Rad\, FG)^x$,*

$$a = (1-g)^x \Big(\sum_{i=0}^{p^m - x - 1} b_i g^i \Big).$$

From Proposition 2.2 it follows that $\{(1-g)^x g^i\}\, 0 \leq i \leq p^m - x - 1$ is a basis of $(Rad\, FG)^x$ and therefore $Dim_F (Rad\, FG)^x = p^m - x$.

Theorem 2.3 *Let F be a field of characteristic p. Let $\mathcal{C}$ be a cyclic code of length p^n and dimension $t \in \mathbb{N}^*$, Let $a = p^n - t$. We consider the p-expansion of the number a: $a \in \{1, ..., p^n - 1\}$,*

$$a = \alpha_1 p^{n-1} + ... + \alpha_n,$$

where $0 \leq \alpha_1, ..., \alpha_n < p$.

1. *If $\alpha_1 = ... = \alpha_n = p-1$ then $dist\,(\mathcal{C}) = p^n$.*
2. *Otherwise, let α_r be the first of coefficients α_j such that $\alpha_r \neq p-1$. Then*

$$dist\,(\mathcal{C}) = \begin{cases} p^{r-1}(\alpha_r + 1), \, if \;\; \alpha_{r+1} = ... = \alpha_n = 0, \\ p^{r-1}(\alpha_r + 2), \, otherwise. \end{cases}$$

Proof $\mathcal{C}$ is a cyclic code of length p^n over the field F, then $\mathcal{C}$ is an ideal of the group algebra FG where G is a cyclic group of order p^n.
$G =< g \mid g^{p^n} = 1 >$ being a cyclic group of order p^n, from [3, pp. 66-67] it follows that the nontrivial ideals of the group algebra FG are exhausted by the principal ideals $R^j = ((a-1)^j)(j = 1, ..., p^n - 1)$, where $R = (RadFG) = (g-1)FG$. Since $Dim_F (Rad\, FG)^{p^n - t} = t$, therefore $\mathcal{C} = (Rad\, FG)^{p^n - t}$.
To calculate the distance of $(RadFG)^{p^n - t}$, let $a = p^n - t = \alpha_1 p^{n-1} + ... + \alpha_n$ be the p-expansion of the number $a \in \{1, ..., p^n - 1\}$. Applying Berman's theorem we conclude that:

1. If $\alpha_1 = \alpha_2 = ... = \alpha_n = p-1$, then $dist\,(\mathcal{C}) = dist\,((RadFG)^a) = p^n$
2. Otherwise, let α_r be the first of coefficients α_j such that $\alpha_r \neq p-1$. Then
$$dist\,(\mathcal{C}) = dist((RadFG)^a) = \begin{cases} p^{r-1}(\alpha_r+1), if\ \alpha_{r+1} = ... = \alpha_n = 0, \\ p^{r-1}(\alpha_r+2), otherwise. \end{cases}$$ ■

3 Distance of cyclic codes over local artinian rings

In this section, we show that the minimum distance of free cyclic codes of length p^n, where p is a characteristic of the residue field, can be obtained by a very easy way using the results of the preceding section.

Definition 3.1 *Let A be a ring. A linear code $\mathcal{C}$ of length n over A is a submodule of the free module A^m. If $\mathcal{C}$ itself is isomorphic to a free A-module, then we say $\mathcal{C}$ is a free code and we define the dimension of $\mathcal{C}$ to be $dim\,\mathcal{C} = rank_A(\mathcal{C})$.*

In the rest of this paper, we will assume that A denotes a local Artinian ring, $\mathfrak{a}$ its maximal ideal, and $\pi : A \longrightarrow A/\mathfrak{a}$ the natural surjection. Later, we will assume that $A/\mathfrak{a}$ is finite. Elements of A^n will be called vectors. A vector which is an element of a code $\mathcal{C} \subseteq A^n$ will also be called a codeword.

Lemma 3.2 ([2], Lemma 3.2)
Let $k < m$ be integers, and let $f : A^k \hookrightarrow A^n$ be any inclusion. Then f splits. Hence, if $\mathcal{C}$ is a free linear code of length n and dimension k over A and $\pi : A^m \longrightarrow (A/\mathfrak{a})^m$ denotes coordinatewise projection, then $\pi(\mathcal{C}) = \mathcal{C}/\mathfrak{a}\mathcal{C}$.

Theorem 3.3 ([2], Theorem 3.4)
Let $\mathcal{C}$ be a linear code over A and $\overline{\mathcal{C}} = \pi(\mathcal{C})$ its coordinatewise projection. Let d and $\overline{d}$ denote the minimum Hamming distances of $\mathcal{C}$ and $\overline{\mathcal{C}}$, respectively. Assume that $\overline{\mathcal{C}} \neq \{0\}$, so that $\overline{d} > 0$. Then

- *1. $d \leq \overline{d}$, and*
- *2. if $\mathcal{C}$ is free, then $d = \overline{d}$.*

Lemma 3.4 *Let A be a local ring, $\mathfrak{a}$ its maximal ideal, and $F = A/\mathfrak{a}$ its residue field. Let M be an-A module. Then $\mu_A(M) = dim_F M/\mathfrak{a}M$ where $\mu_A(M)$ is the number of minimal generators of M.*

Proof : It suffices to prove that

- $(e_1, ...e_n)$ generate $M \Longleftrightarrow (\overline{e}_1, ...\overline{e}_n)$ generate $M/\mathfrak{a}M$ as a $A/\mathfrak{a}$-vector space.

Indeed, if $(e_i)_{i=1,n}$ generate M, then $(\overline{e}_i)_{i=1,n}$ generate $M/\mathfrak{a}M$ as a $A/\mathfrak{a}$-vector space. Conversely if $(\overline{e}_i)_{i=1,n}$ generate $M/\mathfrak{a}M$, then $N + \mathfrak{a}M = M$ where N is the submodule of M generated by (e_i). Since $\mathfrak{a} = \mathrm{Rad(A)}$, using Nakayama we find that $N = M$ and therefore $(e_i)_{i=1,n}$ generate M. Furthermore, if M is free with rank n and $(e_i)_{i=1,n}$ be a minimal system of generators of M, then $(\overline{e}_i)_{i=1,n}$ is a minimal system of generators of the $A/\mathfrak{a}$-vector space $M/\mathfrak{a}M$. Thus $(\overline{e}_i)_{i=1,n}$ is a basis of $M/\mathfrak{a}M$ and $rank_A(\mathcal{C}) = \mu_A(M) = dim_F M/\mathfrak{a}M$. ∎

We give the next theorem which called (The singleton bound) in the case of linear codes over finite field.

Theorem 3.5 *If $\mathcal{C}$ is free of parameters $[n, k, d]$, then $n - k \geq d - 1$.*

Proof It's a consequence of Theorem 3.3 and Lemma 3.4.

Definition 3.6 *A linear code $\mathcal{C}$ of length n over A is cyclic if any cyclic shift of a codeword of $\mathcal{C}$ is a codeword of $\mathcal{C}$, i.e., if $(c_o, c_1, ..., c_{n-1}) \in \mathcal{C}$ then $(c_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$.*

Proposition 3.7 *Let A be an artinian local ring with maximal ideal $\mathfrak{a}$ and residue field $F = A/\mathfrak{a}$ which is finite of characteristic p, let $\mathcal{C}$ be a free cyclic code over A of dimension t, and length p^n. Let $a = p^n - t$. We consider the p-expansion of the number a:*

$$a = \alpha_1 p^{n-1} + ... + \alpha_n, \qquad 0 \leq \alpha_1, ..., \alpha_n < p,$$

for $a \in \{1, ..., p^n - 1\}$.

1. *If $\alpha_1 = ... = \alpha_n = p - 1$ then $dist(\mathcal{C}) = p^n$.*
2. *Otherwise, let α_r be the first of coefficients α_j such that $\alpha_r \neq p-1$. Then*

$$dist(\mathcal{C}) = \begin{cases} p^{r-1}(\alpha_r + 1), if\ \alpha_{r+1} = ... = \alpha_n = 0, \\ p^{r-1}(\alpha_r + 2), \text{otherwise.} \end{cases}$$

Proof

$\mathcal{C}$ is a free code over A. If d is the distance of $\mathcal{C}$, then by Theorem 3.3, we have $d = \overline{d}$ where $\overline{d}$ is the distance of $\pi(\mathcal{C}) = \mathcal{C}/m\mathcal{C} = \overline{\mathcal{C}}$.
It is obvious to verify that $\overline{\mathcal{C}}$ is a cyclic code over the field $F = A/\mathfrak{a}$ of length p^n. Then we can calculate its distance by Theorem 2.3. Let $t' = dim(\overline{\mathcal{C}})$ and p the characteristic of the residue field, from Lemma 3.4 it follows that $t' = dim(\overline{\mathcal{C}}) = dim_F \mathcal{C}/\mathfrak{a}\mathcal{C} = \mu_A(\mathcal{C}) = rank_A(\mathcal{C}) = dim_A(\mathcal{C}) = t$. If d the distance of $\mathcal{C}$, it is known that $d = \overline{d}$. Let $a = p^n - t' = p^n - t$ and let

$$a = \alpha_1 p^{n-1} + ... + \alpha_n$$

be the p-expansion of the number a. In the light of Theorem 2.3 we have

1. If $\alpha_1 = ... = \alpha_n = p-1$ then $d = \overline{d} = p^n$.
2. Otherwise, let α_r be the first of coefficients α_j such that $\alpha_r \neq p-1$. Then
$d = \overline{d} = \begin{cases} p^{r-1}(\alpha_r + 1), \; if \; \alpha_{r+1} = ... = \alpha_n = 0, \\ p^{r-1}(\alpha_r + 2), \; otherwise. \end{cases}$ ∎

4 Conclusion and Open Problems

In this paper we show that, for codes over finite rings, we can find some results similar to codes over finite fields. In fact when the code is free over an artinian local ring with finite residue field, then the code has the basic propriety called (The singleton bound). Further, if we consider cyclic codes of length power of p, this enables us to give an exact formula of minimal distance. It has been shown that if $\mathcal{C}$ is a free cyclic code of length p^n, then the minimum Hamming distance can be calculate in very easy way using the p-expansion of the number $p^n - t$, where t is the dimension of the cyclic code.

In this work we have studied free cyclic codes over an artinian local ring of length p^n where the prime p is the characteristic of the residue field. Now it is naturel to ask what we can say if the cyclic code has length different from p^n ?

ACKNOWLEDGEMENTS. The author is greatly indebted to the referee for his/her useful suggestions.

References

[1] S. Berman, "On the theory of group codes", *Kibernetica*, Vol. 3, (1967), pp. 31-39.

[2] Judy L. Walker, "Algebraic geometric codes over rings", *Journal of Pure and Applied Algebra, 144*, (1999), pp. 99-110.

[3] B. Huppert and N. Blackburn, *Finite groups II*, Springer-Verlag, New York, (1982).

[4] K. Zimmermann, "The weight distribution of indecomposable cyclic codes over 2- groups", *Combinatorial Theory*, Series A 60, (1992), pp. 85-103.

[5] F. J. Mac Williams and N. J. A. Sloane, *The theory of error-corecting codes*, Third printing North-Holland Mathematics Library Vol. 16, (1981).

[6] J. H. Van Lint, *Introduction to coding theory*, GTM 86, Springer-Verlag, New York Second edition, (1991).