Journal of Mathematics and System Science 7 (2017) 261-268
doi: 10.17265/2159-5291/2017.09.003

Maximal codes

Mohammed. Sabiri

ABSTRACT: In this work we try to introduce the concept of Maximal codes that are built over rings, more precisely we will give Maximal codes for special rings, Namely that the notion of maximal codes has been used by Chritophe Chapote, these maximal codes are constructed over finite fields, and these codes are used for coding and decoding.

Key Words: cyclic codes, dual code, noetherian local ring, maximal codes.

1. Introduction

Codes over finite rings are an important class of codes. This is why the study of codes over rings has become an increasingly important area in coding theory. Many of the results of coding theory over finite fields have been extended to codes over finite rings, It is for this reason that we try to introduce the notion of maximal codes over finite rings.
This notion has been studied by Christophe Chabot. For a complete description of codes over finite fields, maximal codes have been shown to have many interesting application to coding and decoding theory (see [3]).
In this paper, we shall generalize this concept over finite commutative rings. We will prove that the set of linear codes constructed over finite ring form equivalence classes, based on the fact that any linear code can be included in a maximal code. The problem of maximal codes is a problem of the search for the maximal ideals in a ring. For this reason, we will give the form of a maximal ideal of the direct sum of a finite number of rings.
In the following, one will be interested in a important class of codes that are the $\mathbb{Z}_{p^m}$- maximal cyclic codes and we will give maximal codes and their dual codes over $\mathbb{Z}_{p^m}$.

2. Rings

We assume that all rings in this paper are commutative with identity.
We begin with some definitions for codes over rings.

Definition 2.1 *Let A be a ring. A linear code $\mathcal{C}$ of length n over A is a submodule of the free module A^n. And the elements of $\mathcal{C}$ are called the words of the code. If more $\mathcal{C}$ is a sub A- free module of rank k, then $\mathcal{C}$ is said a $[n, k]$-code of A and k is called the dimension of the code $\mathcal{C}$.*

Example 2.1 *Soit $A = \mathbb{Z}/4\mathbb{Z}$ et*

$$C = \{(00), (10), (20), (30), (20), (12), (22), (32)\}$$

As in the case of A is a field, it defines the inner product of two elements $a = (a_1, ..., a_n)$ and $b = (b_1, ..., b_n)$ of A^n by:

$$a.b = \sum_{i=0}^{n-1} a_i b_i,$$

The operations being carried out in A, this inner product allows to define a notion of duality on A and it was:

Definition 2.2 *(**dual Code**) Let $\mathcal{C}$ be a linear code on A, then*

$$\mathcal{C}^{\perp} = \{a \in A^n \mid : (\forall b \in \mathcal{C})(a.b = 0)\},$$

is a linear code of length n on A called the dual code of the code $\mathcal{C}$.

Definition 2.3 *A linear code $\mathcal{C}$ of length n over A is cyclic if :*

a- $\mathcal{C}$ is linear,

b- 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 $(c_{n-1}, c_0, ..., c_{n-2}) \in \mathcal{C}$.

As is customary, A_n will denote the ring $\frac{A[X]}{X^n-1}$ and the elements of A_n will be identified with polynomials over A of degree $\leq n-1$. Also, an n-tuple $(c_o, c_1, ..., c_{n-1})$ in A^n will be identified with the element $(c_o + c_1X^{n-1} + ... + c_{n-1}X^{n-1})$ of $A_n = \frac{A[X]}{X^n-1}$. Using this identification, it is easy to see that the cyclic A-codes correspond precisely to the ideals of A_n.

3. Preliminary

Definition 3.1 *Let A be a ring and let M be an A module. A submodule N of an $A-$module M is said to be maximal if N is different from M and if there is no P submodule stuck strictly between N and M.*

Definition 3.2 *An $A-$module is said of finite type if it is generated by a finite number of elements.*

Proposition 3.1 *Let M be an $A-$module of finite type and $L \subset M$ a strict submodule of M. Then there exists a submodule N containing L and maximal.*

Proof: See [5, prop 4, p 30] □

Definition 3.3 *An $A-$module M is said to be noetherian if any increasing sequence of submodules of M is stationed from a certain rank.*

Proposition 3.2 *Let A be a ring.*
Given an $A-$module M, the following three assertions are equivalent :
(A) M is noetherian.
(B) Any non-empty set of submodules of M has a maximal element for inclusion.
(C) Every submodule of M is of finite type.

Proof: See [4, prop3.1, p 40] □

Proposition 3.3 *Let A be a ring.*
Let M be an A-module and $n \in \mathbb{N}$. If M is noetherian, then M^n is noetherian.

Proof: See [5, cor 1, p 22] □

4. Maximal elements of family

We consider a noetherian ring A and an naturel integer n. Let $\mathfrak{N}$ be a family of submodules of A^n. We require that $A^n \in \mathfrak{N}$.
we provide this family with the most natural relation of order, inclusion $\subset$. We obtain a partially ordered family $(\mathfrak{N}, \subset)$

Definition 4.1 *Let C an element of $\mathfrak{N} \setminus A^n$, C is called a maximal element of $\mathfrak{N}$ if*

$$C \subset D \text{ and } D \in \mathfrak{N} \Longrightarrow (D = C \text{ or } D = A^n)$$

In other words N is a maximal element of $\mathfrak{N}$ if there is no submodule between N and A^n.

Theorem 4.1 *Let $\mathfrak{N}$ be a family of submodules of A^n, then $\mathfrak{N}$ admits a maximal element.*

Proof: -The ring A is noetherian, so it is the same for A^n, $\mathfrak{N}$ is a family of submodules of A^n which is notherian then it admits a maximal element. □

Definition 4.2 *We note $\mathcal{N}_{max} = \{N_i\}_{i \in I}$ the set of maximal elements of $(\mathfrak{N}, \subset)$*

Remark 4.1 *If $\mathfrak{N}$ is not reduced to A^n, $\mathfrak{N}$ has at least an maximal element.*

5. Maximal elements of codes

Let A be a finite ring, $\mathfrak{C}$ be the set of sub-modules (codes) of A^n, which can be provided with an inclusion relation and $\mathcal{C}_{max}$ be the set of maximal elements of $(\mathfrak{C}, \subset)$.

Remark 5.1 *-Note that since $\mathfrak{C}$ is a finite family, the number of maximal elements of $\mathfrak{C}$ is finite then $\mathcal{C}_{max} = \{C_i, ..., C_r\}$.*

Proposition 5.1 *Let C an element of $\mathfrak{C}$ $(C \neq A^n)$, then, there exists $i \in \{1, \ldots, r\}$ such that $C \subset C_i$*

Proof:
Let C be an element of $\mathfrak{C}$, then it is a submodule A^n. The A-module A^n is notherian, C is a submodule of A^n so it is of finite type, by applying the Proposition 3.1 C is contained in a maximal submodule of A^n.

□

Conclusion
Any linear code over A is contained in a maximal code.

Definition 5.1 *Let C an element of $\mathfrak{C}$, the signature is defined by*

$$I(C) := \{i \in \{1, \dots, r\} | C \subset C_i\}$$

For any family, $I(A^n) = \emptyset$ and $I(C_i) = \{i\}$.

regroup all elements with the same signature and consider the following set
$\mathfrak{C}_I := \{C \in \mathfrak{C} \,|\, I(C) = I\}$

Proposition 5.2 *Let $\mathfrak{C}$ be the set of linear codes of length n over A.*

The $\mathfrak{C}_I$ defined above form a partition of $\mathfrak{C}$.

$$\mathfrak{C} = \bigcup_{j=1}^{m} \mathfrak{C}_{I_j}$$

Proof:
We consider the following relation :
Let $C_1, C_2 \in \mathfrak{C}$, $C_1 \, R \, C_2 \Longleftrightarrow I(C_1) = I(C_2)$.
It is clear that R is an equivalence relation.
The class of an element C is none other than $\mathfrak{C}_I$.
Therefore $\mathfrak{C}$ is a disjoint finite union of $\mathfrak{C}_I$ □

6. Maximal ideals of $A_1 \oplus A_2$

Theorem 6.1 *Let A_1, A_2 be two rings. Then any maximal ideal of $A_1 \oplus A_2$ is a sum of two ideals I_1 and I_2, where one of the factors is an ideal maximal and the other is equal to A_i.*

Proof: Show that the condition is necessary.
Let I be an maximal ideal of $A_1 \oplus A_2$. Since I is an ideal of $A_1 \oplus A_2$, then $I = I_1 \oplus I_2$, where I_1 and I_2 are two ideals of A_1 et A_2 respectively.
Assume that I_1 is different from A_1 and I_2 is different from A_2.
Then $A_1 + I_2$ is a proper ideal containing $I_1 \oplus I_2$ therefore $I_1 \oplus I_2$ is not a maximal ideal, For this reason we have I_1 is equal to A_1 or I_2 is equal to A_2, for example it is assumed that $I_1 = A_1$, then $I = A_1 + I_2$.
Let us show that I_2 is a maximal ideal of A_2.
If I_2 is not a maximal ideal then it is contained in a maximal ideal M_3 of A_2. So the ideal $A_1 + M_3$ is a proper ideal containing I which is not possible because I is a maximal ideal therefore I_2 is a maximal ideal.
The condition is sufficient because if $I = A_1 + I_2$ where I_2 is a maximal ideal of A_2 or $I = I_1 + A_2$ where I_1 is a maximal ideal of A_1. Then it is easy to show that I is a maximal ideal. □

Corollary 6.1A *Let A_1, $A_2, \dots A_n$ be n rings. Then any maximal ideal of $A_1 \oplus A_2 \oplus \cdots \oplus A_n$ is of the form $M_1 \oplus M_2 \oplus \dots \oplus M_n$ where one of the factors M_i is a maximal ideal of A_i and $M_j = A_j$ for j different from i.*

Proof:
The proof is by induction on i.

7. Maximal codes for cyclic codes over ring A

Let $\mathfrak{C}'$ be the set of cyclic codes of length n over A, we provide this family with the most natural relation of order, inclusion $\subset$. We obtain a partially ordered family $(\mathfrak{C}', \subset)$ □

Theorem 7.1 *Let A be a ring and Let C be a cyclic code of length n over the ring A, so it is contained in a maximal cyclic code.*

Proof: C is a cyclic code of length n on A so it is an ideal of the ring $A_n = \frac{A[X]}{X^n-1}$, but by Krull's Theorem it is contained in a maximal ideal which is also a cyclic code, hence the result. □

Conclusion
Each cyclic code over A is contained in a maximal cyclic code.

Definition 7.1 *Let C an element of $\mathfrak{C}'$, the signature is defined by*

$$I(C) := \{i \in \{1, \ldots, r\} | \, C \subset C_i\}$$

For any family, $I(A^n) = \emptyset$ and $I(C_i) = \{i\}$.

regroup all elements with the same signature
$\mathfrak{C}_I := \{C \in \mathfrak{C}' | I(C) = I\}$

Proposition 7.1 *Let $\mathfrak{C}'$ be the set of cyclic codes of length n over A.*

The $\mathfrak{C}'_I$ defined above form a partition of $\mathfrak{C}'$.

$$\mathfrak{C}' = \bigcup_{j=1}^{r} \mathfrak{C}_{I_j}$$

Proof:
It is the same proof given in Proposition 5.2 □

8. Maximal cyclic codes over $\mathbb{Z}_{p^m}$

Let p be a prime integer that does not divide the integer n and $\mathbb{Z}_{p^m}$ the ring of integers modulo p^m. A unitary polynomial $f(X) \in \mathbb{Z}_{p^m}[X]$ is said to be basic irreducible if its image in $\mathbb{Z}p[X]$ is irreducible.
A cyclic code of length n on the ring $\mathbb{Z}_{p^m}$ is an ideal of the ring $\frac{\mathbb{Z}_{p^m}[X]}{(X^n-1)}$.
For a $\mathbb{Z}_{p^m}$-code C we shall use $C^\perp$ to denote the dual (orthogonal) code of C. For a polynomial f of degree k, f^* will denote its reciprocal polynomial $X^k f(X^{-1})$.

Theorem 8.1 *If $f(X) \in \mathbb{Z}_{p^m}[X]$ is a basic irreducible polynomial then the ideals of $(\mathbb{Z}_{p^m}[X]/(f(X))$ are precisely* (0), $(1+(f(X)))$, $(p+(f(X))), ..., (p^{m-1}+(f(X)))$.

Proof:
See [2, prop 6.6, p 49] □

Recall that $(p + (f(X)))$ is the maximal ideal of $(\mathbb{Z}_{p^m}[X]/(f(X))$

Theorem 8.2 *Any maximal ideal of $\frac{\mathbb{Z}_{p^m}[X]}{(X^n-1)}$ is of the form $M_1 \oplus M_2 \oplus ... \oplus M_r$ such that one of the terms $M_i = (p\widehat{f_i} + (X^n - 1))$ and for j different from i $M_j = \widehat{f_j} + (X^n - 1))$*

Proof: Let p be a prime such that p does not divide n. Let $X^n - 1 = f_1 f_2 \dots f_r$ be the representation of $X^n - 1$ as a product of basic irreducible pairwise-coprime polynomials in $(\mathbb{Z}_{p^m}[X])$.
Let C be a maximal ideal of the ring $R_n = \frac{\mathbb{Z}_{p^m}[X]}{(X^n-1)}$. Then by the Chinese Theorem,

$$R_n = \frac{\mathbb{Z}_{p^m}[X]}{\cap_{i=1}^{r}(f_i)} \simeq \oplus \sum_{i=1}^{r} \frac{\mathbb{Z}_{p^m}[X]}{(f_i)} = \frac{\mathbb{Z}_{p^m}[X]}{(f_1)} \oplus \dots \oplus \frac{Z_{p^m}[X]}{(f_r)}.$$

I is a maximal ideal of the sum $\frac{\mathbb{Z}_{p^m}[X]}{(f_1)} \oplus \dots \oplus \frac{Z_{p^m}[X]}{(f_r)}$, by applying the corollary 6.1A then $C = \oplus \sum_{i=1}^{r} M_i$ where one of the factors M_i is a maximal ideal of $A_i = \frac{\mathbb{Z}_{p^m}[X]}{(f_i)}$ and $M_j = \frac{\mathbb{Z}_{p^m}[X]}{(f_j)}$ for j different from i.
M_i is a maximal ideal of the ring then $A_i = \frac{\mathbb{Z}_{p^m}[X]}{(f_i)}$. Then according to the Theorem 8.1 $M_i = (p + (f_i))$. But $M_i = (p + (f_i))$ correspond to $(p\widehat{f_i} + (X^n - 1))$ in R_n and $M_j = \frac{\mathbb{Z}_{p^m}[X]}{(f_j)}$ correspond to $(\widehat{f_i} + (X^n - 1))$ in R_n.
Consequently C has the following form

$$C = (\widehat{f_1} + (X^n - 1)) \oplus ... \oplus (\widehat{f_{i-1}} + (X^n - 1)) \oplus (p\widehat{f_i} + (X^n - 1)) \oplus ... \oplus (\widehat{f_r} + (X^n - 1))$$

□

Theorem 8.3 *Let p be a prime such that p does not divide n. Let $X^n - 1 = f_1 f_2 \dots f_r$ be the representation of $X^n - 1$ as a product of basic irreducible pairwise-coprime polynomials in $\mathbb{Z}_{p^m}[X]$. Then any maximal cyclic $\mathbb{Z}_{p^m}$-code C is generated by $\{f_i, p\widehat{f_i}\}$; ie.,*

$$C = (f_i, p\widehat{f_i})$$

Where $\widehat{f_i} = \prod f_j (_{1 \le j \le r,\, j \ne i})$.

Proof:
As observed above, $X^n - 1 = f_1 f_2 ... f_r$ are unique basic irreducible pairwise-coprime polynomials. For each i, $1 \le i \le r$, let $\widehat{f_i}$ denote the product of all f_j

different from f_i. Then by application of Theorem 8.2, C is a sum of ideals of the type $(\widehat{f_1})$, $(\widehat{f_2}), .., (\widehat{f_{i-1}})$, $(p\widehat{f_i})$, $(\widehat{f_{i+1}}), ..., (\widehat{f_r})$.
Consider the ideal $\mathcal{C}$ generated by $\{f_i, p\widehat{f_i}\}$ that is to say $\mathcal{C} = (f_i, p\widehat{f_i})$.
For j different from i, f_i divides $\widehat{f_j}$, it follows that $(\widehat{f_j}) \subseteq (f_i)$. Thus the code C is included in $\mathcal{C}$.
Also, since $\widehat{f_i}$, f_i is a pair of coprime polynomials, then $\mathcal{C} = (f_i) \oplus (p\widehat{f_i})$.
There fore,

$$\begin{aligned} |\mathcal{C}| &= |(f_i)||(p\widehat{f_i})| \\ &= p^{m(n-deg(f_i))}p^{(m-1)(n-deg(\widehat{f_i}))} \\ &= p^{m(deg(\widehat{f_i}))}p^{(m-1)(deg(f_i))} \\ &= p^{m(deg(\widehat{f_i}+deg(f_i))}p^{-(deg(f_i))} \\ &= p^{mn-deg(f_i)} \end{aligned}$$

On the other hand, we have the cardinal of the code C is

$$|(\widehat{f_1})||(\widehat{f_2})|, .., |(\widehat{f_{i-1}})||(p\widehat{f_i})||(\widehat{f_{i+1}})|...|(\widehat{f_r})|$$

$$= p^{m(n-deg(\widehat{f_1}))}p^{m(n-deg(\widehat{f_2}))} \dots p^{m(n-deg(\widehat{f_{i-1}}))}p^{(m-1)(n-deg(\widehat{f_i}))}p^{m(n-deg(\widehat{f_{i+1}}))} \dots p^{m(n-deg(\widehat{f_r}))}$$

$$= p^{m\,deg(f_1)}p^{m\,deg(f_2)} \dots p^{m\,deg(f_{i-1})}p^{(m-1)\,deg(f_i)}p^{m\,deg(f_{i+1})} \dots p^{m\,deg(f_r)}$$

$$= p^{m(\,deg(f_1)+deg(f_2)+...+deg(f_{i-1})+deg(f_i)+deg(f_{i+1})+...+deg(f_r))}p^{-deg(f_i)}$$
$$= p^{mn-deg(f_i)}$$

Consequently C is equal to $\mathcal{C}$.

□

Example 8.1 *For $R = \mathbb{Z}/4\mathbb{Z}$ and $n = 7$, we have $X^7 - 1 = g_1(X)g_2(X)g_3(x)$ in $\mathbb{Z}/4\mathbb{Z}$, with $g_1(X) = x - 1$, $g_2(X) = X^3 + 2X^2 + X - 1$, and $g_3(X) = X^3 - X^2 + 2X - 1$, Then by applying Theorem 8.3 we have three maximal codes whose generators are given in the following table*

Table 1: Environments

Code number	The generator polynomials of maximal codes	The single-element generator polynomials
1	$(g_1, 2g_2g_3)$	$g_1 \oplus 2g_2g_3$
2	$(g_2, 2g_1g_3)$	$g_2 \oplus 2g_1g_3$
3	$(g_3, 2g_1g_2)$	$g_3 \oplus 2g_1g_2$

.

Theorem 8.4 *Suppose p is a prime not diving n and C be a maximal cyclic $\mathbb{Z}_{p^m}$-code.*

$$C = (f_i, p\widehat{f_i})$$

Where $\widehat{f_i} = \prod f_j(_{1\leq j\leq r,\, j\neq i})$. *Then*

$$C^{\perp} = p^{m-1}\widehat{f_i}^{*}$$

Proof:

For a finite ring R, it has been shown by (Wood, 1999) [6] that $|C||C^{\perp}| = |R|^n$, if R is a Frobenius ring and where $|R|$ denotes the cardinal of R. Moreover it is shown that every finite chain ring is a Frobenius ring.
The ring $\mathbb{Z}_{p^m}$ is a of frobenius ring and C is a linear code over $\mathbb{Z}_{p^m}$ then we have $|C||C^{\perp}| = |R|^n$.
Therefore, if the code C has p^k codewords and the dual code is of the form p^l then $p^{k+l} = p^{mn}$.
Let $C_1 = p^{m-1}\widehat{f_i}^{*}$. Note that $(f_i)(p^{m-1}\widehat{f_i}^{*})^*$ is divisible by $X^n - 1$ and $(p\widehat{f_i}))(p^{m-1}\widehat{f_i}^{*})^*$ is divisible by p^m. Thus $(f_i)(p^{m-1}\widehat{f_i}^{*})^* = (p\widehat{f_i}))(p^{m-1}\widehat{f_i}^{*})^* = 0\,(mod\, X^n - 1)$.
Consequently $C_1 \subseteq C^{\perp}$.
Also $|C_1| = p^{deg(f_i)}$ and
$|C| = p^{m(n-deg(f_i))}p^{(m-1)(n-deg(\widehat{f_i}))} = p^{m(n-deg(f_i))}p^{(m-1)(deg(f_i)} = p^{mn-deg(f_i)}$.
On the other hand, $|C^{\perp}| = p^l$, where $mn - deg(f_i) + l = mn$. it follows that $l = deg(f_i)$. Hence, $C^{\perp} = C_1$.

□

9. Bibliography

References

1. F. J. Mac Williams and N. J. A. Sloane, *The Theory of Error-Corecting Codes*, Third printing North-Holland Mathematics Library (1981), Volume 16.
2. Parmod Kanwar and Sergio R. Lpez-Permouth, *Cyclic codes over the integrs modulo p^m, Finite fields and their applications*, Vol. 3, pp. 334-352 (1997)
3. Christophe CHABOT, *Reconnaissance de codes, structure des codes quasi-cycliques*, thesis N 29-2009
4. Charles W. Curtis, Irving Reiner, *Representation theory of finite groups and associative algebras*, Pure and Applied Mathematics, Vol. XI, Interscience Publishers (John Wiley Sons), 1962.
5. Nicolas Bourbaki, *Algbre. Chapitre 8 : Modules et anneaux semi-simples*, Actualits scientifiques et industrielles, n 1261, Hermann, 1958.
6. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math. 121 (3) (1999) 555-575.