An-Najah National University

Faculty of Graduate Studies

On Cyclic Z_{p^m}-Codes

By

Ali Saleh Hussein Shaqlaih

Supervisors: Dr. Ali Abdel-Mohsen

Dr. Mohammad A. Saleh

Submitted In Partial Fulfillment of The Requirements for the Degree of Master of Science In MATHEMATICS, Faculty Of Graduate studies, At An-Najah National University At Nablus, Palestine.

2000

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

On Cyclic Z_{p^m}-Codes

By

Ali Saleh Hussein Shaqlaih

Date: 18-7-2000

This thesis was successfully defended on July 18th, 2000 and approved by:

	Committee Members	Signature
1.	Dr. Ali Abdel-Mohsin Mohammad	
2.	Dr. Mohammad Ali Saleh	
3.	Dr. Hasan Yousef	
4.	Dr. 'Mohammad Othman' Omran	

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

To:

Those who taught me patience and diligence:

My father…. and the soul of my mother….

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Acknowledgement:

First of all, thank ***God The Almighty*** for all the blessings He bestowed on me, and continues to bestow.

I wish to extend my gratitude and appreciation to my supervisors: Dr. Ali Abdel-Mohsen, An-Najah N. University, and Dr. Mohammad Saleh, Birzeit University, for their help and advice during the preparation of this thesis.

Thanks are also due to the examiners Committee: Dr. Mohammad Omran, An-Najah N. University, and Dr. Hasan Yousef, Birzeit University, for their valuable suggestions.

I would also like to thank all the lecturers and professors in the department of Mathematics, at An-Najah National University.

My deepest gratitude and appreciation are devoted to López-Permouth, and Vera Pless, for their help providing me with their researches.

Thanks would also be expressed to Fadi Makhlouf for his great efforts in printing this thesis.

Gratitude and thanks to Fr. Emil Salayta, the General Director, and all my colleagues, at the Latin Patriachate Schools in Palestine.

Finally, I would like to express my utmost appreciation to my family, and my friends for all kinds of support, keen interest and concern.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Contents:

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

ABSTRACT:

In this thesis, cyclic codes, their generators, their idempotents, and their dual have been studied. Also, coding and decoding of cyclic codes and Algorithm for decoding linear cyclic codes were under focus.

Moreover, cyclic Z_{p^m} codes, their generators, their dual and their idempotents have been deeply discussed.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

INTRODUCTION:

The beginning of coding theory goes back to the middle of this century with the work of Golay, Hamming and Shannon. Although it has its origins in engineering and applied problems, the subject has been developed by using more mathematical techniques. Mathematical background was at the beginning very little, but as time passes, many mathematical tools, such as group theory, ring theory, and linear programming have been applied to coding theory. Thus, coding theory has now become an active part of mathematical research.

In many cases, the information to be sent is transmitted by a sequence of zeros and ones called binary codes, which means that the code is defined on the field {0, 1}. In other cases, we can define codes over finite rings such as Z_4, Z_8, ...

Z. Qian and V. Pless in [12] have studied cyclic Z_4 codes, their dual generators, and their idempotents. In [7], Kanwar and López-Permouth generalized the results of Pless and Qian from cyclic Z_4-codes to cyclic Z_{p^m}-codes.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

In this thesis, we discuss cyclic codes and cyclic Z_{p^m} codes where p is prime and m is an integer. The material of this thesis lies in three chapters.

CHAPTER I: includes basic concepts, definitions, an introduction to detecting and correcting of error patterns, dual of linear codes, and some algebraic topics that we need in this thesis such as finite fields.

CHAPTER II: includes a study of a class of codes called cyclic codes. In particular, generating polynomials, check polynomials, idempotents and dual cyclic codes have been studied. Also, some important families of cyclic codes like Hamming codes and quadratic residue codes have been studied in this chapter.

CHAPTER III: includes some basic definitions and properties of the ring $Z_{p^m}/\langle x^n-1\rangle$. Local rings, regular polynomials, basic irreducible polynomials, primary ideals and other concepts that will be used in proving theorems for cyclic Z_{p^m} codes have been discussed. Properties of cyclic Z_{p^m} codes, their generator polynomials, the dual and self-dual of Z_{p^m} cyclic codes and their idempotents have also been discussed.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

CHAPTER I

PRELIMINARIES

1.1 Introduction to Coding Theory:

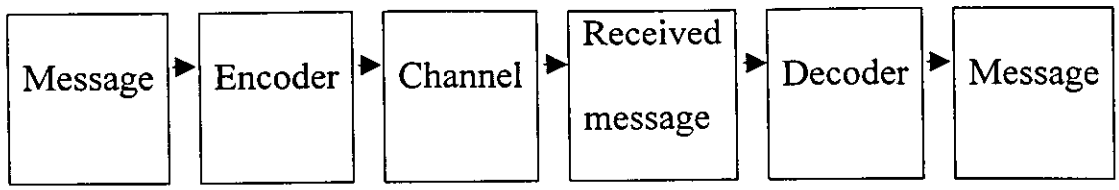
Coding theory is one of the sciences that have been developed recently to suit the increasing need for the safe and pure communications. As some say, coding theory is the science of studying information integrity. It entered the scene to ensure the correction of messages transmitted from one place to another, whether it is inside a computer, compact disk or outside to make our radio and television work properly as communication devices. The subject of error-correcting codes arose originally in response to practical problems in the reliable communication of digitally encoded information. Claude Shannon's paper "A mathematical theory of communication", written in 1948 was the starting of error correcting codes.

We think of a message as a block of symbols from a finite alphabet. A commonly used alphabet is the set of two symbols, 0 and 1. The word is a sequence of digits.

529514

The following diagram shows the steps for sending a message:

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit



The first box contains the message, the message enters the encoder, and in the channel, it changes by noise (may be) then it is received. Then the received message enters the decoder, so the original message can be recovered. To specify what happens:

Suppose that our receiver knows all messages that can be transmitted, say they are C={0000, 1011, 0111, 1100} and we know that in sending the message, one error can happen at most. Then by looking at the received message 1001 we can tell immediately that one error happened since the received message is not in C, and by checking all possible one error message of 1001 we see that the only message that could be sent is 1011. This means that we have detected the error and then we can correct this error.

1.2. Basic definitions for coding theory:

Here, we will define the terminology we will use throughout this thesis.

1.2.1. Definition [5]

A 0 or a 1 is called a digit. A word is a sequence of digits; the length of the word is the number of digits in the word.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.2.2. Example

0110101 is a word of length 7.

1.2.3. Definition [5]

A code C is a nonempty set of words.

1.2.4. Example

$C = \{00, 10, 01, 11\}$ is a code.

1.2.5. Definition [5]

- A block code is a code having all its words of the same length; this number is called the length of a code.
- All codes used in this thesis are block codes.
- The words that belong to a given code C will be called codewords. We shall denote the number of codewords in a code C by $|C|$.

1.2.6. Example

Let $C = \{000, 011, 010, 001\}$, then $|C| = 4$.

1.2.7. Definition [5]

A code of length n, which contains M words will be denoted by $C(n, M)$.

1.2.8. Definition [5]

Let v be a word of length n. The weight of v, denoted by $wt(v)$ is the number of times the digit 1 occurs in v.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.2.9. Example

$wt(110101) = 4, \quad wt(00000) = 0.$

1.2.10. Definition [5]

Let v and w be words of length n. The distance between v and w, denoted by $d(v, w)$, is the number of positions in which v and w disagree.

1.2.11. Example

Let $v = 11010$ and $w = 01101$, then $d(v, w) = 4$.

1.2.12. Definition [15]

- Let K^n be the set of all binary words of length n with addition of words defined componentwise (*mod2*). *i.e.* $0 + 0 = 1 + 1 = 0$, $0 + 1 = 1 + 0 = 1$.
- The scalar multiplication of K^n is defined componentwise and the only scalars are 0 and 1.
- Clearly, K^n is closed under scalar multiplication.
- In the general case, we let F be $GF(q)$ the finite field with q elements.

1.2.13. Theorem [5]

Let v, w and u be words of length n and $a \in \{0, 1\}$, then:

1) $0 \leq wt(v) \leq n$.

2) $wt(v) = 0$ *iff* v is the zero word.

3) $0 \leq d(v, w) \leq n$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

4) $d(v, w) = 0$ *iff* $v = w$.

5) $d(v, w) = d(w, v)$.

6) $d(v, w) = wt(v + w)$.

7) $wt(v + w) \leq wt(v) + wt(w)$.

8) $d(v, w) \leq d(v, u) + d(u, w)$.

9) $wt(av) = a \,.\, wt(v)$.

10) $d(av, aw) = ad(v, w)$.

Proof:

The proofs of (1 – 5) follow immediately from the definition.

For (6 – 10), it follows from the fact that 1 + 1 = 0 in the binary system, so the number of 1's in the word $(v + w)$ is ≤ the number of 1's in v + the number of 1's in w.

1.2.14. Definition [15]

A code C is called linear if $v + w$ is a word in C whenever v and w are in C. That is to say a linear code is a code that is closed under addition of words.

Note that a linear code is a subspace of K^n.

1.2.15. Examples

1) $C_1 = \{000, 111\}$ is a linear code,

since $000 + 000 = 000 \in C$.

$000 + 111 = 111 \in C$.

$111 + 111 = 000 \in C$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2) $C_2 = \{000, 001, 101\}$ is not a linear code, since 001 and 101 are in C_2 but $001 + 101 = 100 \notin C_2$.

1.2.16. Theorem [5]

A linear code must contain the zero word.

Proof:

The proof follows immediately from the fact that $v + v =$ the zero word $\forall\, v \in C$.

1.2.17. Definition [5]

The distance of a code C where $|C| > 1$ is defined to be

$d(C) = min\ \{d(u, v)$: where u and v are distinct codewords in $C\}$.

1.2.18. Example

Let $C = \{01011, 10101, 11101, 10000, 01100\}$, then $d(C) = 1$.

1.2.19. Theorem [5]

If C is a binary linear code, then

$d(C) = min\ \{wt(x) \mid x \in C$ and $x \neq 0\}$.

Proof:

Let $w \neq y \in C$ such that $d(C) = d(w, y)$.

$d(C) = min\ \{d(w, y) \mid w, y \in C$ and $w + y \neq 0\}$.

Then by Theorem 1.2.13 (6)

$d(C) = min\ \{wt(w + y) \mid w, y \in C$ and $w + y \neq 0\}$.

$= min\ \{wt(x) \mid$ for some $x \neq 0\}$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.3. Error -detecting and error- correcting:

1.3.1. Definition [5]

Let C be a code of K^n. If $v \in C$ is sent and $w \in K^n$ is received, then $u = v + w$ is called an error pattern. The code C is said to detect the error pattern u if $v + u$ is not a codeword, $\forall\, v \in C$.

1.3.2. Example

Let $C = \{001, 101, 110\}$.

For the error pattern $u = 010$, we calculate $v + 010$ for all $v \in C$.

$001 + 010 = 011$,

$101 + 010 = 111$,

$110 + 010 = 100$.

None of the three words 011, 111 or 100 is in C, so C detects the error pattern 010.

1.3.3. Example

Let $C = \{001, 101, 110\}$.

For the error pattern $u = 100$, we calculate $v + u$, $\forall v \in C$.

$001 + 100 = 101$,

$101 + 100 = 001$,

$110 + 100 = 010$,

since one of these sums is in C, so C does not detect the error pattern 100.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.3.4. Definition [15]

A code C is t - error detecting if whenever at most t, but at least one error is made in a code word, the resulting word is not a code word. A code C is exactly t-error-detecting if it is t-error detecting but not $(t + 1)$ error-detecting.

1.3.5. Theorem: [15]

A binary code C is exactly t-error detecting if and only if $d(C) = t + 1$.

Proof:

Let u be a nonzero error pattern with $wt(u) \leq d - 1$ and let $v \in C$. Then, $d(v, v + u) = wt(v + v + u) = wt(u) < d$

Since C has distance d, $v + u$ is not in C,

hence C detects u. From the definition of d there are codewords x and y in C with $d(x, y) = d$.

Consider the error pattern $u = x + y$.

Now $y = x + u$ is in C, so C will not detect the error pattern u of weight d. Hence $t = d - 1$

1.3.6. Example

Let $C = \{000, 111\}$, then $d(C) = 3$.

By theorem 1.3.5, C detects all error patterns of weight 1,2 and C does not detect the error pattern of weight 3.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.3.7. Definition [15]

A code C is t-error- correcting if the minimum distance decoding is able to correct all errors of size t or less in any codeword, assuming that all ties are reported as errors. A code C is exactly t-error correcting if it is t-error correcting, but not $(t + 1)$ –error correcting.

1.3.8. Definition [15]

We say that C corrects the error pattern u, if for all v in C, $v + u$ is closer to v than to any other codeword in C.

1.3.9. Example

Let $C = \{000, 111\}$.

Let the error pattern $u = 010$

For $v = 000$

$d(000, v + u) = d(000, 010) = 1$, $d(111, v + u) = d(111, 010) = 2$.

For $v = 111$

$d(000, v + u) = d(000, 101) = 2$, $d(111, v + u) = d(111, 101) = 1$.

Thus C corrects the error pattern 010.

Now take the error pattern $u = 110$,

For $v = 000$, $d(000, v + u) = d(000, 110) = 2$,

$d(111, v + u) = d(111, 110) = 1$

Since $v + u$ is not closer to $v = 000$ than to 111, C does not correct the error pattern 110.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

We describe a procedure called maximum likelihood decoding or *MLD* for deciding which word v in C was sent.

1.3.10 Definition (MLD) [8]

If there is only one word v in C closer to the received word w than any word in C, we decode w as v. If there are more than one word v in C at the same distance from w, we then choose one of these words arbitrary.

1.3.11. Theorem [15]

A code C is t-error-correcting if and only if $d = d(C) = 2t + 1$ or $2t + 2$.

Proof:

Suppose that $d\ (C) = 2t + 1$ or $2t + 2$. And suppose that the received word v differs from the original codeword c in at most t positions, that is $d\ (v,c) \leq t$. Then v is closer to c than to any other codeword, for if $d\ (v, u) \leq t$, for some $u \in C$, then we have, by the triangle inequality. $d\ (c, u) \leq d\ (c, v) + d\ (v, u) \leq t + t = 2t < d(C)$ which contradicts the minimality of d. Hence minimum distance decoding will correct t or fewer errors. Furthermore, if $d(C) = 2t + 1$, then there are codewords c and u for which $d(c, u) = 2t + 1$.

So c and u differ in exactly $2t + 1$ positions. Suppose that the codeword c is sent and that the received word v differs in exactly $t + 1$ positions, all of which are located in the aforementioned $2t + 1$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

positions, and that v now agrees with u in those $t + 1$ error positions.

Thus $d(v, c) = t + 1$, but $d(v, u) = 2t + 1 - (t + 1) = t$

And so maximum likelihood decoding would decode v as u which is incorrect. Hence C is not $(t + 1)$ error –correcting and similarly for if $d(C) = 2t + 2$. For the converse, if C is t –error-correcting, we could not have $d(c, u) \leq 2t$, then it would be possible for the received word v to have precisely t errors, placing it as close to u as to the codeword c, that was originally sent. Hence $d(C) \geq 2t + 1$.

On the other hand, if $d(c) \geq 2t + 3 = 2(t + 1) + 1$, then the code C would be $(t + 1)$ error correcting. Hence $d(C) = 2t + 1$ or $2t + 2$.

1.3.12. Corollary

For any code C, $d(C) = d$ if and only if C is exactly $[(d - 1)/2]$ – error-correcting, where the $[x]$ means the greatest integer of x.

Proof:

Follows from Theorem 1.3.11.

1.4. Generator and parity check matrices:

1.4.1. Definition [5]

If $u = (u_1, u_2, \ldots, u_n)$ and $v = (v_1, v_2, \ldots, v_n)$ are two vectors in a vector space V over $GF(p)$, p: Prime, then the inner product of u and v is

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

$u.v = \sum_{i=1}^{n} u_i v_i (\text{mod } p)$. If $u.v = 0$, we say that u and v are orthogonal to each other. Note for $p = 2$, (orthogonality) means that u, v have an even number of 1's in common.

1.4.2. Definition [5]

Note that a linear code C spans a subspace of K^n with dimension k. Any matrix whose rows form a basis for C is called a generator matrix for C.

The generator matrix for C is $k \times n$ matrix, and it must have rank k.

Proof:

Follows from the definition of the generator matrix.

1.4.3. Theorem [15]

A $k \times n$ matrix G is a generator matrix for some linear code C if and only if the rows of G are linearly independent, that is, if and only if the rank $(G) = k$.

Proof:

The proof follows immediately from the definition.

1.4.4. Theorem [11]

If G is a generator matrix for a linear code C, then any matrix row equivalent to G is also a generator matrix for C.

Proof: Follows from the properties of row operations.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.4.5. Example

$C = \{0000, 1110, 0111, 1001\}$.

To find the generator matrix for C we change A to *RREF*[*] by elementary row operations:

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

So $G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ is a generator matrix for C.

1.5 Dual of linear codes:

1.5.1. Definition [8]

Let C be a (n, k) code. Then the dual code $(C^{\perp})$ of C is $C^{\perp} = \{u \in K^n \mid u \,.\, w = 0, \ \forall\, w \in C\}$.

1.5.2. Algorithm

We illustrate an algorithm for finding $C^{\perp}$ for the code C.

1) Form the matrix A whose rows are the words in C.

2) Use elementary row operations to write A in *RREF*.

[*] RREF: Reduced Row Echolon Form.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3) Let G be the $k \times n$ matrix consisting of all the nonzero rows of the *RREF* of A.

4) Let X be the $k \times (n-k)$ matrix obtained form G by deleting the leading k columns of G.

5) Form the following $n \times (n-k)$ matrix $H = \begin{bmatrix} X \\ I_{n-k} \end{bmatrix}$

6) The columns of H form a basis for $C^{\perp}$.

1.5.3. Example

If S = {11101, 10110, 01011, 11010}. To find $C^{\perp}$ we apply algorithm 1.5.2.

$$A = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\longrightarrow \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$\Rightarrow G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, k = 3 \text{ and } X = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \end{bmatrix}$$

The leading columns of G are columns 1, 2 and 3, so the rows of x are placed in rows 1,2 and 3 respectively of the 5 × 2 matrix H.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

So $H = \begin{bmatrix} 0 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$

$\Rightarrow$ The basis for $C^{\perp}$ is the columns of H, or the rows of H^T.

1.5.4. Theorem [8]

a) If G is a generator matrix for C, then $C^{\perp} = \{x \in K^n \mid xG^T = 0\}$

b) The dual $C^{\perp}$ of the linear (n, k) code is a linear $(n, n\text{-}k)$ code.

c) $(C^{\perp})^{\perp} = C$ for any linear code C.

Proof:

a) Since x is orthogonal to every codeword in C if and only if it is orthogonal to every codeword in a basis for C.

b) Follows from the definition of dual code.

c) Let $w \in C \Rightarrow x.w = 0 \ \forall x \in C^{\perp}$, then

$w \in (C^{\perp})^{\perp} \Rightarrow C \subset (C^{\perp})^{\perp}$ but C and $(C^{\perp})^{\perp}$ have the same dimension, and so they must be equal.

1.5.5. Definition [8]

A linear code C for which $C = C^{\perp}$ is said to be self–dual.

1.5.6. Example

$C = \{0000, 1100, 0011, 1111\}$.

C is self-dual. Note that C is a $C(4, 2)$ code, since $C \subset C^{\perp}$ and $C^{\perp}$ is also (4,2) code. So $C^{\perp} = C$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.5.7. Definition [11]

A matrix H is called a parity-check matrix for a linear code C if the columns of H form a basis for the dual code $C^{\perp}$.

1.5.8. Theorem [11]

If H is a parity-check matrix for a linear code C of length n, then C consists precisely of all words v in K^n such that $vH = 0$.

Proof:

The proof follows immediately from the fact that the columns of the parity check matrix form a basis for $C^{\perp}$.

1.5.9. Theorem [15]

If matrices G and H are generator and parity-check matrices respectively for some linear code C then:

1) The rows of G are linearly independent.
2) The columns of H are linearly independent.
3) The number of rows of G + the number of columns of H = the number of columns of G which equals the number of rows of H.
4) $GH = 0$.

Proof: Follows from the definition of G and H.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.5.10. Theorem [5]

If H is a parity check matrix of C then H^T (transpose of H) is a generator matrix for $C^{\perp}$.

Proof:

Let G and H be the generator matrix and the parity check matrix respectively for C, then $H^T G^T = (GH)^T = 0$. Thus $(GH)^T = 0$. Hence H^T is a generator matrix for $C^{\perp}$.

1.5.11. Definition [15]

If C is any code of length n, then the code L of length n which is obtained by choosing a particular permutation of n digits and then consistently rearranging every word in C in the chosen way. L is said to be equivalent to C.

1.5.12. Example

Let $C = \{11111, 01111, 00111, 00110, 00010\}$, $n = 5$

We choose to rearrange the digits in the order 2, 1, 4, 5, 3 then

$L = \{11111, 10111, 00111, 00101, 00100\}$. L is equivalent to C.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.6 Syndrome decoding:

1.6.1. Definition [8]

If C is a linear code and if u is a code word in K^n, then the coset of C determined by u is the set of all words of the form $v + u$ as v ranges over all codewords in C. We denote this coset by $C + u$, thus $C + u = \{v + u \mid v \in C\}$.

1.6.2. Example

Let $C = \{000, 111\}$. And let $u = 101$.

Then $C + 101 = \{000 + 101, 111 + 101\} = \{101, 010\}$.

1.6.3. Theorem [5]

Let C be a linear code of length n. Let u and v be words of length n.

1) If u is in the coset $C + v$, then $C + u = C + v$, that is each word in a coset determines that coset.
2) The word u is in the coset $C + u$.
3) If $u + v$ is in C, then u and v are in the same coset.
4) If $u + v$ is not in C, then u and v are in different cosets.
5) If C has dimension k, then there are exactly 2^{n-k} different cosets of C, and each coset contains exactly 2^k words.
6) Two cosets are either disjoint or coincide.

Proof: Follows from the properties of cosets.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.6.4. Definition [5]

If C is a linear code, and v is a word then the word of the least weight in the coset is called a coset leader.

1.6.5. Definition [15]

Let C be a linear code of length n and dimension k. Let H be a parity check matrix for C. For any word w in K^n, the syndrome of w(denoted by syn(w)) is the word wH in K^{n-k}.

1.6.6. Example

Let $C = \{0000, 1011, 0101, 1110\}$. Let $w = 1101$

By algorithm 1.5.2, we can find H to be

$$H = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\Rightarrow wH = 1101 \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix} = 11 = \text{syn}(w)$$

1.6.7. Theorem [11]

Let C be a linear code of length n. Then

1) Every word in a fixed coset has the same syndrome.

2) Words in different cosets have different syndromes.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Proof:

1) Let $v + C$ be a coset of C, let $v + c_1$, $v + c_2$ be any two words in the coset C for some $c_1, c_2 \in C$ and suppose the parity check matrix for C is H, then $(v + c_1)H = vH = (v + c_2)H$.

   $\Rightarrow$ The two words have the same syndrome.

2) Let u and v be two different words in two cosets and have the same syndrome, then $uH = vH \Rightarrow (u.v)H = 0 \Rightarrow u.v \in C$. So v and u are in the same coset, which is a contradiction.

1.6.8. Theorem: [8]

1) The syndrome of w, $\text{syn}(w) = wH$ is zero if and only if w is a code word of C.
2) There is a 1 – 1 correspondence between syndromes and cosets.
3) If no errors occur, and if w is the received word, then the syndrome of w is zero but not conversely.

Proof:

1. Follows from Theorem 1.5.8.
2. Follows from the properties of syndromes and cosets.
3. Suppose no errors occur, then w will be a codeword and by (1), $syn(w) = wH = 0$.

Notice that (from Theorem 1.6.7.) we can identify a coset by its syndrome; the syndrome of a coset is the syndrome of any word in the coset.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

We are now ready to define syndrome decoding. We choose a set of coset leaders of an (n, k) code C and list them with their syndromes. Since all the words in a coset have the same syndrome, this list contains all possible 2^{n-k} syndromes.

In practice, we do not have to write down a standard array. The code itself has the zero word as its syndrome, and we can use the zero word as coset leader. We can then choose words of weight 1 as coset leaders. We compute their syndromes, whenever we get a new syndrome, we have a new coset leader, we go on to see if words of weight 2 can be coset leaders. Thus, each time we get a new syndrome, we put it in the list with the coset leader of weight i that gave rise to it. After we complete the words of weight i, we continue with words of weight $i + 1$ until we reach our 2^{n-k} syndromes.

To decode a received word w, compute syn (w); locate this in the syndrome list, subtract the coset leader u corresponding to this syndrome from w. decode w as $w - u = x$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.6.9. Example

Let C = {0000, 1011, 0101, 1110}, we calculate the parity check matrix H to be

$$H = \begin{bmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{bmatrix}$$

And we find the syndromes for the coset leader in the following table:

Coset leader u	**Syndrome uH**
0000	00
1000	11
0100	01
0010	10

Assume that w = 1101 is received. Then the syndrome is wH = 11, which gives a coset leader u = 1000 (see the table). We conclude that $x = w + u = 0101$ was sent.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.7 Finite Fields:

1.7.1. Definition [10]

A commutative ring with unity is called a field if every nonzero element is a unit.

1.7.2. Definition [10]

The order of a field is the number of elements in the field. If the order is infinite, we call the field an infinite field, and if the order is finite, we call the field a finite field.

1.7.3. Example:

1) Z_5 is a finite field.

2) $\Re$ is infinite field.

1.7.4. Definition: [10]

If F is a field and a is an element in F, the least positive integer n for which $a^n = 1$ is called the order of a.

Now, we state the following theorems without proofs.

1.7.5. Theorem [10]

If p is a prime number and n is a positive integer, then there is (up to isomorphism) exactly one field of order $q = p^n$ which is denoted by F_q or $GF(q)$. Furthermore, all finite fields have size p^n, for some prime number p and positive integer n.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1.7.6. Theorem [11]

Let a be an element in a field F. If a has order n, then $a^m = 1$, if and only if m is a multiple of n.

1.7.7. Theorem [1]

If a is an element of order r in a field F, then a^s has order $r/\ g.c.d\ (s,\ r)$. where $g.c.d\ (s,\ r)$ is the greatest common divisor of s and r.

1.7.8. Theorem [1]

If a is an element that has order n in a field F and b has order m with $g.c.d\ (m,\ n) = 1$, then ab has order mn.

1.7.9. Definition [1]

We say that a is a primitive n^{th} root of unity if and only if the order of a is n. In a field of order q, we say a is a primitive field element if and only if the order of a is $q - 1$.

1.7.10. Theorem [11]

Every finite field has a primitive element.

1.7.11. Theorem [11]

Every element in a field of order q satisfies the equation $x^q - x = 0$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

CHAPTER II

CYCLIC CODES OVER FINITE FIELDS

2.1 Introduction:

One of the most important classes of linear codes is the class of cyclic codes. These codes have great practical importance and they are also of considerable interest from an algebraic point of view since they are easy to encode. They also include the important family *Bose-Chadhuri-Hocquengham (BCH)* codes which is of great practical importance for error correction, particularly the number of errors is expected to be small compared with the length of the code. Also cyclic codes are considered important since they are the building blocks for many other codes.

2.1.1 Definition [5]

Let v be a word of length n, the cyclic shift π (v) of v is the word of length n obtained from v by taking the last digit of v and moving it to the beginning, all other digits moving one position to the right. *i.e.* $(v_0,.....,v_{n-1}) \xrightarrow{\pi} (v_{n-1},v_0,.....,v_{n-2})$.

2.1.2 Example

Let $v = 10110$, then $\pi(v) = 01011$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.1.3 Definition [5]

A code C is said to be cyclic if the cyclic shift of each codeword is also a codeword, *i.e.* whenever $(v_0, v_1, v_2, \ldots\ldots, v_{n-1}) \in C$, then so is $(v_{n-1}, v_0, \ldots\ldots, v_{n-2})$.

2.1.4 Example

Let $C_1 = \{000, 110, 101, 011\}$

C_1 is a linear cyclic code since $\pi\ (v) \in C$, $\quad \forall\, v \in C$

Let $C_2 = \{000, 100, 011, 111\}$

C_2 is not cyclic code since $\pi\ (100) = 010 \notin C$.

2.1.5 Lemma [5]

The cyclic shift (π) is a linear transformation over $\{0, 1\}$, that is if v, w are two words, then $\pi\ (v + w) = \pi\ (v) + \pi\ (w)$ and

$\pi\ (a\, v) = a\ \pi\ (v) \qquad \forall\, a \in \{0,1\}$

Proof: Trivial.

If we wish to construct a cyclic linear code, then we pick a word v and form a set S consisting of v and all of its cyclic shifts, *i.e.* $S = \{v, \pi(v), \pi^2(v), \ldots, \pi^{n-1}(v)\}$, where $\pi^n(v) = \pi(\pi(\pi \ldots \pi(v))$ n times, and define C to be the linear span of S that is $C = \langle S \rangle$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.1.6 Example

Let $n = 3$, $v = 100$. Thus $S = \{ v, \pi(v), \pi^2(v)\}$

$S = \{100, 010, 001\}$ generates a cyclic code.

2.1.7 Definition [2]

A polynomial of degree n over a field K is $a_0 + a_1x + ... + a_nx^n$, where the coefficients $a_0,....,a_n$ are elements of K. The set of all polynomials over K is denoted by $K[x]$.

Polynomials over K are added and multiplied in the usual fashion except that since $1 + 1 = 0$, we have $x^k + x^k = 0$. Note that the degree of $f(x) + g(x)$ need not be max $\{deg\, f(x), deg\, g(x)\}$.

2.1.8 Example

Let $n = 8$, and $f(x) = 1 + x + x^3 + x^4$, $g(x) = x + x^2 + x^3$. Then,

$f(x) + g(x) = 1 + x^2 + x^4$, $f(x)\, g(x) = (1 + x + x^3 + x^4)\,(x + x^2 + x^3) = x + x^7$.

2.2 Generator polynomial for a cyclic code:

Cyclic codes have a good representation in terms of polynomials. If the word v corresponds to the polynomial $v(x)$, then the cyclic shift of v , $\pi(v)$, corresponds to the polynomial $xv(x)\ mod\ (1+x^n)$.

If $v = (v_0, ..., v_{n-1})$, we define the polynomial $v(x)$ coresponding to v by $v(x) = v_0 + v_1x + ... + v_{n-1}x^{n-1}$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Note that $v = (v_{n-1}, v_0, \ldots\ldots, v_{n-2})$ corresponds to $v_{n-1} + v_0x + \ldots. + v_{n-2}x^{n-1} = v_0x + \ldots\ldots + v_{n-2}x^{n-1} \bmod (1 + x^n) = xv(x) \bmod (1 + x^n)$.

2.2.1 Example

$v_1 = 100$, corresponds to $v_1(x) = 1$, $\pi(v_1) = 010$ corresponds to $xv_1(x) = x$. $v_2 = 1101$ corresponds to $v_2(x) = 1 + x + x^3$, $\pi(v_2) = 1110$ corresponds to $xv_2(x) \bmod (1 + x^4) = 1 + x + x^2$.

2.2.2 Lemma [5]

Let C be a cyclic code, and let $v \in C$, then for any polynomial $a(x)$, $c(x) = a(x)\, v(x) \bmod (1+x^n)$ is a codeword in C.

Proof:

Clearly, if $c(x) \in <\{v(x), xv(x), \ldots\ldots, x^{n-1}v(x)\}> (mod\ 1+x^n)$. then this means that: $c(x) = (a_0v(x) + a_1xv(x) + \ldots\ldots + a_{n-1}x^{n-1}v(x)) \bmod 1+x^n$.

$= (a_0 + a_1x + a_2x^2 + \ldots\ldots + a_{n-1}x^{n-1})\, v(x) \bmod 1+x^n$.

$= a(x)v(x) \bmod 1+x^n$. Thus the proof is complete.

2.2.3 Definition [11]

A nonempty subset I of a ring $\Re$ is called an ideal of $\Re$ if:

(i) $a, b \in I$ implies $a - b \in I$

(ii) $a \in I$ and $r \in \Re$ imply $ar \in I$ and $ra \in I$.

2.2.4 Definition [10]

All polynomials in $K[x]$ of degree less than n with multiplication modulo $(x^n - 1)$ will be denoted by:

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

$\Re_n$ *i.e.* $\Re_n = K[x] / \langle x^n - 1 \rangle$

2.2.5 Theorem [11]

A set of elements S in $\Re_n$ corresponds to a cyclic code C if and only if S is an ideal in $\Re_n$.

Proof:

Suppose S is a set of elements in $\Re_n$ that generates a cyclic code. Then if $a_1(x)$ and $a_2(x)$ are in S, so are $a_1(x) \pm a_2(x)$.

Recall that the cyclic shift corresponds to multiplication by x, so that if $a(x)$ is in S, then $a(x)x$ is in S, as is $(a(x)x)x = a(x)x^2$, and so on. Consider $a(x)\, b(x)$ for $a(x)$ in S and $b(x) = b_0 + b_1x + b_2x^2 \ldots + b_{n-1}x^{n-1}$, some polynomial in $\Re_n$. Then $a(x)\, b(x) = b_0\, a(x) + b_1\, a(x) + \ldots$ $\ldots + b_{n-1}\, a(x)\, x^{n-1}$ is again in S. Hence S is an ideal. Suppose, now, S is an ideal in $\Re_n$, then clearly the polynomials in S correspond to the words in a cyclic code.

2.2.6 Theorem [11]

Let S be an ideal in $\Re_n$, and let $\langle S \rangle = C$, then

1. There is a unique monic polynomial $g(x)$ of minimal degree in C such that $C = \langle g(x) \rangle$ and it is called the generator polynomial for C.
2. The generator polynomial $g(x)$ divides $x^n - 1$.
3. If *deg* $(g(x)) = r$, then C has dimension n-r and $C = \langle g(x) \rangle$ $= \{s(x)g(x) \mid deg\, s(x) < n\text{-}r\}$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

4. If $g(x) = g_0 + g_1x + \text{----} + g_rx^r$, then $g_0 \neq 0$ ($g_0 = 1$) and C has the following generator matrix.

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_r & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & g_0 & g_1 & \cdots & \cdots & \cdots & \cdots & 0 \\ . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ . & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & \cdots & g_0 & g_1 & g_2 & \cdots & g_r \end{bmatrix}$$

Proof:

1. Suppose that C contains two distinct monic polynomials $g_1(x)$ and $g_2(x)$ of minimum degree r. Then their difference $g_1(x) - g_2(x)$ would be a non zero polynomial in C of degree less than r which is not possible. Hence there is a unique monic polynomial $g(x)$ of degree r in C. Since $g(x) \in C$ and C is an ideal, we have $\langle g(x) \rangle \subset C$. On the other hand, suppose that $p(x) \in C$, and let $p(x) = q(x)\, g(x) + r(x)$, where $deg\ (r(x)) < r$, then $r(x) = p(x) - q(x)\, g(x) \in C$ has degree less than r, which is possible only if $r(x) = 0$. Hence $p(x) = q(x)\, g(x) \in \langle g(x) \rangle$, and so $C \subset \langle g(x) \rangle$. Thus $C = \langle g(x) \rangle$.

2. Dividing x^n-1 by $g(x)$ gives $x^n-1 = q(x)g(x) + r(x)$ where $deg\ (r(x)) < r$. Since in $\Re_n$, $x^n-1 = 0 \in C$.

   We see that $r(x) \in C$, and so $r(x) = 0$, which means that $g(x) \mid x^n-1$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3. The ideal generated by $g(x)$ is$<g(x)> = \{f(x)g(x) \mid f(x) \in \Re_n\}$.

   With the usual reduction modulo $x^n - 1$,

   and we must show that it is sufficient to restrict $f(x)$ to polynomials of degree less than $n - r$. We know that $g(x) \mid x^n-1$, and so $x^n-1 = h(x)\, g(x)$ for some $h(x)$ of degree $n-r$. Divide $f(x)$ by $h(x)$ so $f(x) = q(x)h(x) + s(x)$ where $deg\ (s(x)) < n-r$, then $f(x)g(x) = q(x)h(x)g(x) + s(x)g(x) = q(x)(x^n-1) + s(x)g(x)$ and so $f(x)g(x) = s(x)g(x)$ in $\Re_n$, and this shows that the set $\{g(x), xg(x),\ldots., x^{n-r-1}\, g(x)\}$ spans C and since it is linearly independent, it forms a basis for C. Hence $dim\ (C) = n-r$.

4. If $g_0 = 0$, then $g(x) = xg_1(x)$, where $deg(g_1(x)) < r$. But then we would have $g_1(x) = 1.g_1(x) \equiv x^n g_1(x) = x^{n-1}g(x)$

   Hence $g_1(x) \in C$, which contradicts the fact that no nonzero polynomial in C has degree less than r.

   Thus $g_0 \neq 0$. Finally, G is a generator matrix of C since $\{g(x), xg(x),\ldots., x^{n-r-1}\, g(x)\}$ is a basis for C.

2.2.7 Theorem [11]

A monic polynomial $p(x)$ in $\Re_n$ is the generator polynomial for an ideal if and only if $p(x) \mid x^n-1$.

Proof:

($\Rightarrow$) Done by theorem 2.2.6 (2)

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

($\Leftarrow$) Suppose that $p(x) \mid x^n-1$, and let $g(x)$ be the generator polynomial for $C = \langle p(x) \rangle$. Assume that $p(x) \neq g(x)$.

Since $p(x)$ and $g(x)$ are both monic, we must have

deg $(p(x))$ > *deg* $(g(x))$. By assumption, $x^n-1 = p(x)f(x)$ for some polynomial $f(x)$. Furthermore, since $g(x) \in \langle p(x) \rangle$, we have $g(x) \equiv a(x)p(x)$ for some $a(x) \in \mathfrak{R}_n$. Multiplying both sides by $f(x)$ we get

$g(x)f(x) \equiv a(x)p(x).f(x) \equiv a(x)(x^n-1) \equiv 0.$

But *deg* $(g(x)f(x)) <$ *deg* $(p(x)f(x)) = n$, and so $g(x)f(x) = 0$,

which is impossible. Hence $p(x) = g(x)$

2.2.8 Corollary [5]

The generator polynomial $g(x)$ for the smallest cyclic code of length n containing the word v (polynomial $v(x)$) is the greatest common divisor of $v(x)$ and $1 + x^n$. (That is $g(x) =$ g.c.d $(v(x), 1+x^n)$).

Note: By smallest cyclic code, we mean less numbers of codewords.

***Proof*:**

If $g(x)$ is the generator polynomial then $g(x)$ divides both $v(x)$ and $1+x^n$. But $g(x)$ is in $\langle \{v(x), xv(x),\ldots,x^{n-1}v(x)\} \rangle$. Thus we have $g(x) = a(x)v(x)$ *mod* $1+x^n$, or $g(x) = a(x)v(x) + b(x)(1+x^n)$ (by division algorithm). Thus any common divisor of $v(x)$ and $1 + x^n$ must divide $g(x)$, and thus $g(x)$ is the greatest common divisor.

529514

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.2.9 Example

Let $n = 8$ and $v = 11011000$. So $v(x) = 1 + x + x^3 + x^4$.

The g.c.d of $v(x)$ and $1 + x^8$ is $1 + x^2$.

Thus $g(x) = 1 + x^2$. And the smallest linear cyclic code containing $v(x)$ has dimension 6 and $g(x)$ is the generator polynomial.

2.2.10 Theorem [11]

Let C_1, C_2 be cyclic codes with generator polynomials $g_1(x)$, $g_2(x)$, respectively, then:

1. The generator polynomial for $C_1 \cap C_2$ equals *l.c.m.* $(g_1(x), g_2(x))$.
2. The generator polynomial for $C_1 + C_2$ equals *g.c.d* $(g_1(x), g_2(x))$.
3. $C_1 \subseteq C_2$ if and only if $g_2(x) \mid g_1(x)$.

Proof:

We'll only prove (3).

It follows, since $C_1 \subseteq C_2$ *iff* $g_2(x)$ divides $g_1(x)$ *iff* $\langle g_1(x) \rangle \subseteq \langle g_2(x) \rangle$.

2.3 The Check Polynomial:

2.3.1 Definition [15]

Let C be a cyclic $(n, n\text{-}r)$ code with generator polynomial $g(x)$ so $x^n - 1 = g(x)\, h(x)$. Then $h(x)$ is called the check polynomial of C with degree $n - r$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.3.2 Theorem [15]

Let $h(x)$ be the check polynomial for a cyclic code C in $\Re_n$ then

1) The code C can be described by $C = \{p(x) \in \Re_n \mid p(x)h(x) \equiv 0\}$

2) If $h(x) = h_0 + h_1x + h_2x^2 + \ldots + h_{n-r}x^{n-r}$, then the parity check matrix for C is given by:

$$H = \begin{bmatrix} h_{n-r} & \ldots & \ldots & \ldots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_{n-r} & \ldots & \ldots & \ldots & h_0 & 0 & \ldots & 0 \\ . & 0 & h_{n-r} & \ldots & \ldots & \ldots & h_0 & 0 & 0 \\ .. & \ldots & .. & h_{n-r} & \ldots & \ldots & \ldots & h_0 & \ldots \\ \ldots & \ldots & \ldots & \ldots & .. & .. & .. & .. & .. \\ 0 & 0 & 0 & \ldots & \ldots & h_{n-r} & 0 & \ldots & h_0 \end{bmatrix}^T$$

***Proof*:**

Let $g(x)$ be the generator polynomial of C.

1. If $p(x) \in C$, then $p(x) = f(x)g(x)$ for some polynomial $f(x) \in \Re_n$

Hence $p(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) \equiv 0$.

On the other hand, if $p(x) \in \Re_n$ such that $p(x)h(x) \equiv 0$, then we write $p(x) = q(x)g(x) + r(x)$, where $deg\ (r(x)) < r$. Multiplying by $h(x)$ gives $p(x)h(x) = q(x)g(x)h(x) + r(x)h(x)$. Hence, $r(x)h(x) \equiv 0$. However $deg\ (r(x)h(x)) < r + (n - r) = n$, and so we deduce that $r(x)h(x) = 0$, hence $r(x) = 0$ and $p(x) = q(x)g(x) \in C$.

2. If $c(x) \in C$ then $c(x)h(x) \equiv 0$. Thus $deg\ (c(x)h(x)) < 2n\text{-}r$, and from this we deduce that the coefficients of x^{n-r}, x^{n-r+1},..., x^{n-1} *(r times)* in the product $c(x)h(x)$ must be 0, that is:

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

$c_0h_{n-r} + c_1h_{n-r-1} + \ldots + c_{n-r}h_0 = 0$

$c_1h_{n-r} + c_2h_{n-r-1} + \ldots + c_{n-r+1}h_0 = 0$

.

.

$c_{r-1}h_{n-r} + c_rh_{n-r-1} + \ldots + c_{n-1}h_0 = 0$

which is equivalent to $(c_0\ c_1 \ldots . c_{n-1})H^T = 0$. And so, H is the parity check matrix for C.

2.3.3 Example

Let C be a cyclic code of length $n = 9$

$X^9 - 1$ factors over F_2 as $X^9 - 1 = (x^3)^3 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$

$= (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1)$. Take $C = \langle x^6 + x^3 + 1 \rangle$ with generator polynomial

$g(x) = x^6 + x^3 + 1$. Then C has dimension $9 - 6 = 3$. And generator matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

And C has check polynomial $h(x) = \dfrac{x^9 - 1}{g(x)}$

$$= \frac{(x-1)(x^2+x+1)(x^6+x^3+1)}{x^6+x^3+1} = (x-1)(x^2+x+1) = x^3 - 1.$$

So C has the parity check matrix

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{bmatrix}^T$$

2.4 Finding Cyclic Codes:

2.4.1 Definition [5]

A polynomial $f(x)$ in $K[x]$ where K is a field, and degree of $f(x) \geq 1$ is irreducible if it is not the product of two polynomials in $K[x]$, both of which have degree at least one.

To construct a linear cyclic code of length n, and dimension k we must find factors of $1+x^n$.

2.4.2 Example

For $n = 3$, we factorize $1 + x^3 = (1 + x)(1 + x + x^2)$. Thus there are two proper cyclic codes of length 3 one has generator

$g_1(x) = 1 + x$ and generator matrix.

$G_1 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ and the code is $C_1 = \{000, 110, 011, 101\}$.

The other code has generator $g_2(x) = 1 + x + x^2$ and the generator matrix $G_2 = [1 \quad 1 \quad 1]$, with $C_2 = \{000,111\}$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.4.3 Definition [10]

An ideal I in $\Re_n$ is called principal ideal if every element in I is a multiple of a fixed polynomial $g(x)$ *i.e*: If I is principal, then $I = \{c(x)g(x) ; c(x) \text{ in } \Re_n\}$. We denote this by $I = \langle g(x) \rangle$

2.4.4 Definition [10]

A ring is called a principal ideal ring (*P.I.R*) if every ideal in it is principal.

The next theorems tell us how to find cyclic codes and they were proved in 2.2.6.

2.4.5 Theorem [11]

If C is an ideal (*i.e* a cyclic code of length n),

in $\Re_n = K[x] / \langle x^n-1 \rangle$, and $g(x)$ is the monic polynomial of smallest degree in C. Then $g(x)$ is uniquely determined and $C = \langle g(x) \rangle$.

Proof:

We show in this theorem that $\Re_n$ is a *P.I.R* and that the monic generator of smallest degree of an ideal is unique even though an ideal can have other generators. First, we show that $\Re_n$ is a *P.I.R*. Let $g(x)$ be the monic ploynomial of smallest degree in C, and let $a(x)$ be any other polynomial in C. By division algorithm in $F[x]$, $a(x) = g(x)b(x) + r(x)$ where the degree of $r(x)$ is less than the degree of $g(x)$. by the definition of an ideal, $r(x)$ is in C. But this contradicts the

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

choice of $g(x)$ unless $r(x)$ is identically zero, so that $a(x) = g(x)b(x)$. Hence $\mathfrak{R}_n$ is a *P.I.R.* If $g(x)$ and $h(x)$ are monic polynomials of the same degree and both are in C, then $g(x) - h(x)$ is a polynomial in C of lower degree than either. This can't happen if $g(x)$ has the smallest degree. Thus, $g(x)$ is the unique monic polynomial of smallest degree in C, and $C = \langle g(x) \rangle$. And hence the proof is complete.

The following theorem tells us explicitly how to find the generator of a cyclic code.

2.4.6 Theorem [11]

If C is an ideal in $\mathfrak{R}_n$, the unique monic generator, $g(x)$ of C of smallest degree divides x^n-1 and conversely if a polynomial $g(x)$ in C divides x^n-1, then $g(x)$ has the lowest degree in $\langle g(x) \rangle$.

Proof:

Suppose, first that $g(x)$ is monic polynomial of smallest degree in C. By division algorithm in $K[x]$, $x^n - 1 = a(x)g(x) + r(x)$ where the degree of $r(x)$ is less than the degree of $g(x)$.

Now, $r(x) = -a(x)g(x) \ mod \ (x^n - 1)$, and so $r(x)$ is in $\langle g(x) \rangle$. This is a contradiction unless $r(x)$ is identically zero. Thus $g(x)$ divides $x^n - 1$.

Conversely, suppose that $g(x)$ divides $x^n - 1$ and that $b(x)$ is in $\langle g(x) \rangle$ but has lower degree than $g(x)$. Then, $b(x) = c(x)g(x) + (x^n - 1)d(x)$ in

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

$K[x]$ because $b(x)$ is in C. However, since $g(x)$ divides $x^n - 1$, $g(x)$ divides $b(x)$, which is a contradiction. Thus, the proof is complete.

2.5 Encoding and decoding of cyclic codes:

Usually we encode the code as a polynomial generator. The simplest is the $k \times n$ generator matrix in which the rows are the codewords corresponding to the generator polynomial and its first $k-1$ cyclic shifts,

i.e. $G = \begin{bmatrix} g(x) \\ xg(x) \\ \cdot \\ \cdot \\ \cdot \\ x^{k-1}g(x) \end{bmatrix}$

2.5.1 Example

Let $C = \{0000, 1010, 0101, 1111\}$ be a linear cyclic code. The generator polynomial for C is $g(x) = 1 + x^2$. $n = 4$, $k = 2$. So a basis of C is $g(x) = 1 + x^2 \equiv 1010$, $xg(x) = x + x^3 \equiv 0101$. Hence the generator matrix for C is $G = \begin{bmatrix} g(x) \\ xg(x) \end{bmatrix} = \begin{bmatrix} 1+x^2 \\ x+x^3 \end{bmatrix} = \begin{bmatrix} 1010 \\ 0101 \end{bmatrix}$

2.5.2 Definition [15]

Let C be a cyclic code. If $c(x) \in C$ is the codeword sent and $u(x)$ is the received polynomial, then $err(x) = u(x) - c(x)$ is the error polynomial.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.5.3 Definition [15]

Let $C = \langle g(x) \rangle$ be a cyclic $(n,n-r)$ code, the syndrome of a polynomial $u(x)$, denoted by $syn(u(x))$, is the remainder upon dividing $u(x)$ by $g(x)$, that is $u(x) = q(x)g(x) + syn(u(x))$, and $deg\,(syn(u(x)) < r$, where $r = deg\,(g(x))$.

A received polynomial $u(x)$ is a codeword if and only if its syndrome is the zero polynomial.

2.5.4 Example

Let $n=7$ and $g(x) = 1+x+x^3$, so $n-k=3$

We produce the syndrome as follows

Cosets Leader	Syndrome
0	0
1	1
x	x
x^2	x^2
x^3	$x+1$
x^4	x^2+x
x^5	x^2+x+1
x^6	x^2+1

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

If $u(x) = 1 + x + x^6$ is received, we compute its syndrome polynomial $x^6 + x + 1 = (x^3 + x + 1)^2 + (x^2 + x)$. So, $Syn(u(x)) = x^2 + x$. Then from the above table the coset leader is $a(x) = x^4$. And so we decode $u(x)$ as $c(x) = u(x) - a(x) = x^6 + x^4 + x + 1$

2.5.5 An algorithm for decoding linear cyclic codes

Here we state an alogorithim for decoding linear cyclic codes.

1. Calculate the syndrome polynomial $s(x) = w(x)$ *mod* $g(x)$, where w is the received word.
2. For each $i \geq 0$, calculate $s_i(x) = x^i s(x)$ *mod* $g(x)$

(the syndrome polynomial of the cyclic shift of w)

until a syndrome s_j is found with $wt(s_j) \leq t$, then the most likely error polynomial is: $e(x) = x^{n-j} s_j(x)$ *mod*$(1 + x^n)$

2.5.6 Example

Let $n = 15$, and let $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ be the generator polynomial for a cyclic code with distance $d = 5$. Thus all error patterns at weight $t = 2$ or less are correctable. We want to decode the received word $w = 110011100111000$

Here $w(x) = 1 + x + x^4 + x^5 + x^6 + x^9 + x^{10} + x^{11}$.

The syndrome polynomial $s(x) = w(x)$ *mod*$g(x)$ is

$s(x) = 1 + x + x^3 + x^4 + x^5 + x^6 + x^7$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

$s_1(x) = xs(x) = x + x^2 + x^4 + x^5 + x^6 + x^7 + x^8 \ mod g(x)$

$= 1 + x + x^2 + x^5$

$s_2(x) = x^2 s(x) \equiv x + x^2 + x^3 + x^6 \ (mod g(x))$

$s_3(x) = x^3 s(x) \equiv x^2 + x^3 + x^4 + x^7 \ (mod g(x))$

$s_4(x) = x^4 s(x) \equiv 1 + x^3 + x^5 + x^6 + x^7 \ (mod g(x))$

$s_5(x) = x^5 s(x) \equiv 1 + x \ (mod g(x))$ which has weight $2 \leq t$

So, $e(x) = x^{15-5} s_5(x) \ mod \ (1+x^{15}) = x^{10} + x^{11}$. Therefore,

$c(x) = w(x) + e(x) = w(x) + (x^{10} + x^{11}) = 1 + x + x^4 + x^5 + x^6 + x^9$

Thus $c = 110011100100000$.

2.6 Idempotents for linear cyclic codes:

We note that all cyclic codes can be obtained from a factorization of x^n-1 into monic irreducible factors F_q.However factoring x^n-1 is not so easy in general. In fact there are other generators that can be found without factoring x^n-1, and they give another approach to describe cyclic codes. These are called idempotent generators.

2.6.1 Definition [15]

A polynomial $e(x) \in \mathfrak{R}_n$ is said to be idempotent in $\mathfrak{R}_n$ if $e^2(x) \equiv e(x)$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.6.2 Example

In $R_7 = K[x]/\langle x^7-1\rangle$ the polynomial $x^3 + x^5 + x^6$ is an idempotent since $(x^3+x^5+x^6)^2 \equiv x^3+x^5+x^6$.

2.6.3 Definition [15]

A generator $e(x)$ of an ideal in $\Re_n$ is called an idempotent generator if it is an idempotent.

2.6.4 Lemma [15]

Let C be a cyclic code, then

1. The idempotent acts as a unit.
2. If $e_1(x)$, $e_2(x)$ are idempotents, then so is $e_1(x) + e_2(x)$ and $e_1(x)e_2(x)\ (mod\ (x^n + 1))$.

Proof:

Follows from the definition of the idempotent.

2.6.5 Theorem [8]

Let C be a cyclic code in $\Re_n$ with generator polynomial $g(x)$ and check polynomial $h(x)$. Then $g(x)$ and $h(x)$ are relatively prime, and so there exist polynomials $a(x)$ and $b(x)$ for which $a(x)\,g(x) + b(x)\,h(x) = 1$

The polynomial $e(x) = a(x)g(x)mod(x^n\text{-}1)$ has the following properties:

1. $e(x)$ is the unique identity in C, that is $p(x)e(x) \equiv p(x)\ \ \forall\ p(x) \in C$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2. $e(x)$ is the unique polynomial in C that is both idempotent and generates C, that is $C = \langle e(x) \rangle$

Proof:

If $e_1(x)$ and $e_2(x)$ are both identities in $\mathfrak{R}_n$, then,

$e_1(x) \equiv e_1(x)\, e_2(x) \equiv e_2(x)$. And so $e_1(x) = e_2(x)$. Thus if an indentity exists, it is unique since $g(x)h(x) = x^n-1$ has no multiple roots in any extension field, $g(x)$ and $h(x)$ are relatively prime so

$\exists\ a(x), b(x)$ such that $a(x)g(x) + b(x)h(x) = 1$ ..... *

If $p(x) \in C$, then $p(x)h(x) \equiv 0$, and so (*) gives $a(x)g(x)p(x) \equiv p(x)$, which says that $e(x) = a(x)g(x) mod(x^n-1)$ is indeed the identity in C and also that $e(x)$ generates C since any polynomial in C is a multiple of $e(x)$ and since $e(x)$ is an identity, then $e(x)$ is idempotent. To complete the proof, we need only to show that an idempotent $f(x)$ that also generates C must be equal to $e(x)$. Since $f(x)$ generates C, there exists $q(x) \in \mathfrak{R}_n$ for which $e(x) \equiv q(x)f(x)$. Hence, $f(x) \equiv e(x)f(x) \equiv q(x)\, f^2(x) \equiv q(x)f(x) \equiv e(x)$, thus $f(x) = e(x)$.

The previous theorem shows that we can compute $e(x)$ from $g(x)$ using the Euclidean algorithm.

The next Theorem shows how to compute $g(x)$ from $e(x)$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.6.6 Theorem [11]

If $e(x)$ is the idempotent generator of C, then the generator polynomial of C equals $g.c.d\ (e(x), (x^n-1))$.

Proof:

By the previous theorem, since $x^n-1 = g(x)h(x)$ and $e(x) \equiv a(x)g(x)$, we have $g.c.d\ (e(x), x^n-1) = g.c.d\ (a(x)g(x), h(x)g(x))$. But according to the previous theorem $a(x)$, $h(x)$ are relatively prime and so $g.c.d\ (e(x), x^n-1) = g.c.d\ (a(x)g(x), h(x)g(x)) = g(x)$.

2.6.7 Theorem [11]

Let C_1 and C_2 be cyclic codes with corresponding generator polynomials $g_1(x)$ and $g_2(x)$, and corresponding idempotent generators $e_1(x)$ and $e_2(x)$, then

1. $C_1 \cap C_2$ has idempotent generator equals $e_1(x)e_2(x)$.
2. $C_1 + C_2$ has idempotent generator $e_1(x) + e_2(x) - e_1(x)e_2(x)$
3. $C_1 \subset C_2$ if and only if $e_1(x)e_2(x) \equiv e_1(x)$ where all polynomials are taken modulo x^n-1.

Proof:

We prove only (1) and (2):

1. Clearly $e_1(x)\ e_2(x)$ is in $C_1 \cap C_2$ and $(e_1(x)e_2(x))^2 = e_1(x)^2\ e_2(x)^2 = e_1(x)e_2(x)$. So $e_1(x)e_2(x)$ is an idempotent in $C_1 \cap C_2$.

   If $c(x)$ is in $C_1 \cap C_2$, then $e_1(x)e_2(x)c(x) = e_1(x)c(x) = c(x)$.

   So $e_1(x)e_2(x)$ is a unit for $C_1 \cap C_2$ and so generators $C_1 \cap C_2$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2. Clearly $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is in $C_1 + C_2$ and $(e_1(x) + e_2(x) - e_1(x)e_2(x))^2 = e_1(x) + e_2(x) - e_1(x)e_2(x)$.

So $e_1(x) + e_2(x) - e_1(x)e_2(x)$ is an idempotent in $C_1 + C_2$.

If $c(x)$ is in $C_1 + C_2$, then $c(x) = c_1(x) + c_2(x)$ for some $c_1(x)$ in C_1 and for some $c_2(x)$ in C_2.

Hence $(c_1(x) + c_2(x))(e(x) + e_2(x) - e_1(x)e_2(x))$

$= c_1(x)e_1(x) + c_1(x)e_2(x) - c_1(x)e_1(x)e_2(x) + c_2(x)e_1(x) + c_2(x)e_2(x) - c_2(x)e_1(x)e_2(x) = c_1(x) + c_1(x)e_2(x) - c_1(x)e_2(x) + c_2(x)e_1(x) + c_2(x)e_1(x) = c_1(x) + c_2(x)$. So, $e_1(x) + e_2(x) - e_1(x)e_2(x)$ acts as a unit for $C_1 + C_2$ and this generates it.

2.6.8 Definition [11]

An ideal M in a ring R is called a minimal ideal if 0 is the only ideal strictly contained in M.

2.6.9 Theorem [11]

If x^n-1 = $(x$-1$)\ f_1(x).....f_k(x)$ is a factorization of x^n-1 into irreducible factors, then there are $k + 1$ minimal ideals $c_1,....,c_{k+1}$ with generator polynomial $f_1^n(x),....., f_k^n(x), (x^n - 1)$, and idempotent generators $e_1(x),....,e_{k+1}(x)$. These $e_i(x)$ satisfy the following conditions:

1. $e_i(x)\, e_j(x) = 0$ if $i \neq j$

2. $\sum_{i=1}^{k+1} e_i(x) = 1$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Furthermore, any cyclic code C is a sum of minimal ideals C_i. And its idempotent e is the sum of the idempotents e_i for the C_i.

Proof:

Since the C_i are minimal ideals, $C_i \cap C_j = 0$ for $i \neq j$ so that $e_i e_j = 0$ for $i \neq j$ because $e_i e_j$ is in $C_i \cap C_j$. Now $C_1 + C_2$ had idempotent $e_1 + e_2 - e_1 e_2 = e_1 + e_2$, and it can be shown that $C_1 + C_2 + \ldots\ldots + C_{k+1}$ has idempotent $e_1 + e_2 + \ldots\ldots + e_{k+1}$. We know that $C_1 + C_2$ has a generator polynomial equals $g.c.d\ (f_1^n(x), f_2^n(x))$. It follows by finite induction that the generator polynomial of $C_1 + C_2 + \ldots\ldots + C_{k+1}$ equals $g.c.d\ (f_1^n(x), \ldots\ldots, f_k^n(x), (x^n - 1))$. But this $g.c.d$ can only be 1 since that factors are distinct, hence $1 = e_1 + e_2 + \ldots\ldots + e_{k+1}$.

If C is any ideal, then C has idempotent generator $e(x)$.

Hence $e(x) = e(x)\ e_1(x) + \ldots\ldots + e(x)\ e_{k+1}(x)$. The ideal $C \cap C_i$ is contained in C_i and so is either 0 or C_i. If $C \cap C_i = C_i$, then $C_i \subseteq C$ and $ee_i = e_i$, Otherwise $ee_i = 0$. Hence $e(x)$ is the sum of the $e_i(x)$ of those i such that $C_i \subset C$ and C itself is the sum of the C_i that are contained in it.

2.6.10 Theorem [11]

Let $x^n - 1 = g(x)h(x)$ and let C be a cyclic code with generator polynomial $g(x)$ and idempotent generator $e(x)$. Then the code with generator polynomial $h(x)$ has idempotent generator $1 - e(x)$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Proof:

Since $h(x)(1 - e(x)) \equiv h(x)(1 - a(x)g(x)) \equiv h(x)$, we see that $1 - e(x)$ is the identity in $<h(x)>$, and so generates $<h(x)>$.

2.7 Dual Cyclic Codes

Recall that the dual code ($C^{\perp}$) of C is:

$C^{\perp} = \{u \in V \mid u.w = 0, \forall w \in C\}$.

2.7.1 Theorem [8]

If C is a linear cyclic code of length n and dimension k with generator $g(x)$ and if $1 + x^n = g(x)\,h(x)$, then:

$C^{\perp}$ is a cyclic code of dimension $n - k$ with generator $x^k h(x^{-1})$

Proof:

Since C has dimension k, $g(x)$ has degree $n - k$ and thus $h(x)$ has degree k. Since $g(x)\,h(x) = 1 + x^n$, we have $g(x^{-1})\,h(x^{-1}) = (1 + x^{-n})$

and so, $x^n g(x^{-1})\,h(x^{-1}) = x^n(1 + x^{-n})$

$x^{n-k}\,g(x^{-1})\,x^k h(x^{-1}) = 1 + x^n$. Thus $x^k\,h(x^{-1})$ is a factor of $1 + x^n$ having degree k and hence the generator polynomial for the linear cyclic code, $C^{\perp}$ of dimension $n - k$ containing $x^n\,h(x^{-1})$.

2.7.2 Example

Let $n = 7$, and $g(x) = 1 + x + x^3$ is a generator for code C,

So $k = 7 - 3 = 4$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Since $g(x)$ is a factor of $1 + x^7$, we can find $h(x)$ where $1 + x^7 = g(x)\ h(x)$ by long division. In this case, $h(x) = 1 + x + x^2 + x^4$. The generator for $C^{\perp}$ is $g^{\perp}(x) = x^4\ h(x^{-1}) = x^4(1 + x^{-1} + x^{-2} + x^{-4}) = 1 + x^2 + x^3 + x^4$. which corresponds to $1011100 = w$.

Note $g \,.\, w = 0$ and $\pi^k(g).w = 0$. (π is the cyclic shift).

2.7.3 Theorem [13]

Let $x^n - 1 = g(x)h(x)$, and let C be a cyclic code with idempotent generator $e(x)$. Then $C^{\perp}$ has an idempotent generator $1 - e(x^{-1})$.

Proof:

It is clear that $e(x)$ is orthogonal to $(1 - e(x^{-1}))$ and hence $1 - e(x^{-1})$ is in $C^{\perp}$.

2.8 Families of Codes

In this section, we want to list briefly some of the most important families of codes.

2.8.1 Hamming Codes [15]

The Hamming Codes $H_q(r)$ are probably the most famous of all error-correcting codes. The codes were discovered independently by Marcel Golay in 1949 and Richard Hamming in 1950. They are perfect, linear codes that decode in a very elegant manner. In addition, all binary Hamming codes are equivalent to cyclic codes, and some but not all, non-binary Hamming codes are equivalent to

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

cyclic codes. Also, Hamming codes are important family of codes since they are easy to encode and decode.

2.8.2 Definition [15]

A code of length $n = 2^r - 1$, $r \geq 2$, having parity check matrix H whose rows consist of all nonzero vectors of length r is called a Hamming code of length $2^r - 1$.

2.8.3 Example:

One possibility for a parity check matrix for a Hamming code of length 7 ($r = 3$) is:

$$H = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

2.8.4 Definition [15]

Two binary (n, m) codes C_1, C_2 are equivalent if one can be turned into the other by permuting the coordinate positions of each codeword, and by permuting the code symbol in each position of each codeword. *"Recall definition 1.5.11"*.

2.8.5 Theorem [15]

The binary Hamming Code $H_2(r)$ is equivalent to a cyclic code.

Proof: See [15].

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

2.8.6 BCH Codes [15]

An important class of multiple-error-correcting codes is the class of Bose-Chaudhuri-Hocquengham codes or *BCH* codes.

BCH codes are important for two reasons: First, they admit a relatively easy decoding scheme, and, secondly, the class of *BCH* codes is quite extensive.

2.8.7 Definition [15]

Let w be a primitive *n-th* root of unity over F_q, and let $g(x)$ be the monic ploynomial over F_q of smallest degree that has $\delta - 1$ numbers: $w^b, w^{b+1}, \ldots, w^{b+\delta-2}$, among its zeros, where $b \geq 0$ and $\delta \geq 1$.

Thus $g(x) = l.c.m. = \{m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x)\}$.

where $x^n - 1 = \pi_i m_i(x)$.

The *q-ary* cyclic code B_q (n, δ, w, b) of length n, with generator polynomial $g(x)$, is called a *BCH* code with designed distance δ (Note that the designed distance is one greater than the number of zeros).

2.8.8 Quadratic Residue Codes

The quadratic residue codes are another class of cyclic codes that have prime length p.

2.8.9 Definition [15]

An integer a is quadratic residue *mod p* if the equation $x^2 \equiv a$ *mod p* has a solution.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Note that since 2 is quadratic residue *mod p* if and only if p has the form $8m \pm 1$, the binary quadratic residue codes must have prime length of the form $p = 8m \pm 1$.

2.8.10 Definition [15]

The binary quadratic residue codes have prime length of the form $p = 8m \pm 1$ and generator polynomial $g(x)$ may be either:

$q(x) = \prod_{r \in QR} (x - w^r)$ or $n(x) = \prod_{u \in NQR} (x - w^u)$, where

$QR \subset \{1, \ldots, p\text{-}1\}$ is the set of quadratic *mod p*

$NQR \subset \{1, \ldots, p\text{-}1\}$ is the set of quadratic non residues *mod p*.

Note: Since there are precisely $\frac{(p-1)}{2}$ elements in each set QR and NQR, the quadratic residue codes have dimension

$$k = n - \deg(g(x)) = p - \frac{(p-1)}{2} = \frac{p+1}{2}.$$

2.8.11 Example:

Let $p = 7$, the $QR = \{1, 2, 4\}$ and $NQR = \{3, 5, 6\}$. Hence, if w is a primitive 7^{th} root of unity over F_2, then:

$$q(x) = (x - w)(x - w^2)(x - w^4) = x^3 + x + 1$$

and $$n(x) = (x - w^3)(x - w^5)(x - w^6) = x^3 + x^2 + 1$$

Thus $QR(7) = < x^3 + x + 1 >$ is a binary cyclic code.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

CHAPTER III

CYCLIC CODES OVER INTEGERS MODULO p^m.

3.1 Basic concepts

In this section, we write some basic definitions and notations.

3.1.1 Definition [10]

Let $\Re$ be a ring, M an additive abelian group and $(r, m) \longrightarrow rm$ be a mapping from $\Re \times M$ into M, such that:

1) $r(m_1 + m_2) = rm_1 + rm_2$.

2) $(r_1 + r_2)m = r_1m + r_2m$.

3) $(r_1r_2)m = r_1(r_2m)$.

4) $1\, m = m$ *if* $1 \in \Re$.

$\forall\, r,\ r_1,\ r_2 \in \Re$ and $\forall\, m,\ m_1,\ m_2 \in M$. Then M is called a left $\Re$–module.

3.1.2 Example

Let A be any additive abelian group, then A is left Z-module.

3.1.3 Definition [10]

A nonempty subset N of an $\Re$–module M is called an $\Re$–submodule of M if:

1) $a - b \in N \quad \forall\ a, b \in N.$ 2) $ra \in N \quad \forall\ a \in N, r \in \Re.$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.1.4 Definition

A subset C of $Z^n_{p^m}$ is called a Z_{p^m} - code if C is a Z_{p^m} - submodule of $Z^n_{p^m}$.

3.1.5 Notation

In this chapter $\Re_n$ will denote the ring $Z_{p^m}[x] / (x^n-1)$ and the elements of $\Re_n$ will be identified with polynomials of degree $\leq n-1$. Also, an *n-tuple* $(a_0, a_1,.....,a_{n-1})$ in Z_{p^m} will be identified with the element $a_0 + a_1x + ... + a_{n-1}x^{n-1}$ of $\Re_n$.

3.1.6 Definition [6]

For a polynomial f of degree k, f^* will denote its reciprocal polynomial $x^k f(x^{-1})$.

3.1.7 Definition [10]

A polynomial $f \in Z_{p^m}[x]$ is called nilpotent if there exists a positive integer n such that $f^n = 0$.

3.1.8 Definition [7]

A polynomial $f \in Z_{p^m}[x]$ is called regular if it is not a zero divisor, *i.e.* if for $g \in Z_{p^m}[x], fg = 0$, then $g = 0$.

3.1.9 Definition [7]

A commutative ring $\Re$ is called local if it has a unique maximal ideal.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.1.10 Example

Z_{p^m} is a local ring with unique maximal ideal pZ_{p^m}.

3.1.11 Lemma [7]

A commutative ring $\Re$ (with 1) is local if and only if for every $a \in \Re$ either a or $1 - a$ is invertible.

3.1.12 Definition [7]

By $\mu : Z_{p^m}[x] \to Z_p[x]$, we will denote the ring homomorphism that maps $a + (p^m)$ to $a + (p)$ and the variable x to x.

3.1.13 Definition [9]

If f is in $\Re$ $[x]$, then f is a unit if there is a polynomial h with $fh = 1$.

3.1.14 Lemma [7]

If $f \in Z_{p^m}[x]$, then

1. f is a unit if and only if μf is a unit .
2. f is regular if and only if $\mu f \neq 0$.
3. f is regular if and only if f is not nilpotent.

Proof: See [7].

3.1.15 Definition [9]

If $f \in \Re$ $[x]$, then f is irreducible if f is not a unit and whenever $f = gh$, then g or h is a unit for some h, g in $\Re$ $[x]$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.1.16 Definition [10]

A commutative integral domain $\Re$ with unity is called a unique factorization domain (or briefly, a *UFD*) if it satisfies the following conditions.

(i) Every nonunit of $\Re$ is a finite product of irreducible factors.

(ii) Every irreducible element is prime.

3.1.17 Example

The ring of integers Z is a *UFD*.

3.2 The ring $\Re_n$

In order to find generator polynomials of a Z_{p^m} – code, we need to know the structure of the ring $\Re_n = Z_{p^m}[x]/ (x^n-1)$.

3.2.1 Definition [14]

An ideal I in a ring is a primary ideal if $xy \in I$ implies $x \in$ I or $y^k \in I$, for some integer k.

3.2.2 Definition [9]

Two polynomials f and g in $Z_{p^m}[x]$ are called coprime if $Z_{p^m}[x] = (f) + (g)$.

3.2.3 Lemma [7]

If f and g are coprime and $f|gh$ then $f|h$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.2.4 Theorem [7]

If $f, g \in Z_{p^m}[x]$ are regular then f, g are coprime if and only if μf, μg are coprime.

Proof:

Let f and g be coprime, then there exist f_1, $g_1 \in Z_{p^m}[x]$ such that $1 = ff_1 + gg_1$. Also $\mu f \neq 0 \neq \mu g$ and $1 = \mu f \mu f_1 + \mu g \mu g_1$ and so μf, μg are coprime. Conversely, if μf and μg are coprime, then there exist f_1, g_1 and r in $Z_{p^m}[x]$ such that

$f(x) f_1(x) + g(x) g_1(x) = 1 + p^k r(x)$, for some positive integer k.

Since $1 + p^k r(x)$ is invertible in $Z_{p^m}[x]$, it follows that $1 \in (f) + (g)$ and so f and g are coprime.

3.2.5 Definition [9]

We say that a polynomial f in $Z_{p^m}[x]$ is basic irreducible if μf is irreducible in $Z_p[x]$.

3.2.6 Definition [7]

We say f is primary if (f) is a primary ideal. That is if $gh \in (f)$ implies that either $g \in (f)$ or $h^k \in (f)$ for some positive integer k.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.2.7 Definition [9]

J will denote the set of all those $f \in Z_{p^\infty}[x]$ such that μf has no repeated roots in the algebraic closure of Z_p.

Now we state Hensels' Lemma to use it in proving the next theorem.

3.2.8 Theorem (Hensels' Lemma) [9]

Let f be in $\Re_n$ and $\mu f = \bar{g}_1 \ldots\ldots \bar{g}_n$, where $\bar{g}_1 \ldots\ldots \bar{g}_n$ are pair-wise coprime. Then there exist $g_1 \ldots\ldots g_n$ in $\Re_n$ such that:

1. $g_1 \ldots\ldots g_n$ are pair-wise coprime.
2. $\mu g_i = \bar{g}_i \quad , \ 1 \le i \le n.$
3. $f = g_1 \ldots\ldots g_n$.

3.2.9 Theorem [9]

Suppose f is a regular polynomial in $Z_{p^\infty}[x]$, then:

1. If f is basic irreducible then f is irreducible.
2. If f is irreducible then $\mu f = ug^n$, where u is a unit, g is a monic irreducible polynomial in $Z_p[x]$, and $n \in Z^+$.
3. If $f \in J$ then f is irreducible if and only if f is basic irreducible.

Proof:

1. Suppose that f is regular in $Z_{p^\infty}[x]$, and f is basic irreducible (μf is irreducible). Then, if $f = gh$ either μg or μh is a unit by

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Lemma 3.1.9 g or h is a unit. Thus if μf is irreducible (f is basic irreducible) then f is irreducible.

2. Let f be irreducible in $Z_{p^m}[x]$, and suppose $\mu f = u g_1^{e1}, \ldots . g_t^{et}$, where u is a unit and the g_i are monic irreducible coprime polynomials in $Z_p[x]$. Then, unless $t = 1$, By Hensels' Lemma f factors non-trivially. That is, if f is irreducible then $\mu f = u g^n$ where u is a unit in $Z_p[x]$ and g is irreducible.

3.2.10 Theorem [7]

If f is a basic irreducible polynomial in $Z_{p^m}[x]$, then f is primary.

Proof:

Suppose $g(x)\, h(x) \in (f(x))$. Since f is basic irreducible, so $\mu f(x)$ is irreducible in $Z_p[x]$, so $g.c.d\,(\mu f(x), \mu g(x)) = 1$ or $\mu f(x)$. If $g.c.d\,(\mu f(x), \mu g(x)) = 1$ then by (theorem (3.2.4)) f and g are coprime.

Thus $1 = f(x) f_1(x) + g(x)\, g_1(x)$ for some $f_1(x), g_1(x) \in Z_{p^m}[x]$, so that $h(x) = f(x)h(x)f_1(x) + g(x)h(x)g_1(x)$. Since $g(x)h(x) \in (f(x))$ it follows that $f(x) \mid h(x)$. If $g.c.d\,(\mu f(x), \mu g(x)) = \mu f(x)$, then there exist $u(x)$, $v(x) \in Z_{p^m}[x]$ such that $g(x) = f(x)\, u(x) + p^k v(x)$ for some positive integer $k < m$. But then $g^m(x) \in (f(x))$, and hence f is primary.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

We know that, if $\Re$ is a local ring, the polynomial ring $\Re[x]$ may not be a unique factorization domain. But some special polynomials $\Re[x]$ may have the unique factorization property. An example of such polynomials is regular polynomials.

For regular polynomials in a polynomial ring $\Re[x]$ over a local ring $\Re$, we have the following theorem.

3.2.11 Theorem [9]

Let f be a regular polynomial in $\Re[x]$. Then

1. $f = ug_1g_2....g_k$, where u is a unit and $g_1,g_2,....,g_k$ are regular, primary, pair-wise – coprime polynomials.
2. If $f = ug_1g_2.....g_k = vh_1h_2.....h_L$, where u, v are units and $\{g_i\}$, $\{h_i\}$ are families of regular primary, pairwise–coprime polynomials, then $k = L$ after renumbering $(h_i) = (g_i)$, $1 \le i \le k$.

Proof:

For (1) Let f be regular in $\Re[x]$. Then $\mu f \neq 0$

Thus $\mu f = \bar{u}\bar{\pi}_1^{h_1} .....\bar{\pi}_n^{h_n}$, where $\bar{u}$ is a unit and $\bar{\pi}_1,.....,\bar{\pi}_n$ are irreducible coprime polynomials in $k[x]$ -($Z_p[x]$)-.

By (theorem 3.2.8) – (Hensels' Lemma) –

529514

$f = u\ \pi_1.....\pi_n$, where $\mu u = \bar{u}$ and $\mu\pi_i = \bar{\pi}_i^{h_i}$

So π_i are regular primary coprime polynomials.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

For (2) Interms of principal ideals if $(g_1).....(g_k) = (h_1).....(h_L)$ where the $\{(g_i)\}$ and $\{(h_i)\}$ are regular primary coprime ideals, then $n = m$ after a suitable ordering $(g_i) = (h_i)$, $1 \le i \le n$.

In our case the local ring is Z_{p^m}, and so any polynomial has at least one coefficient that is not divisible by p is regular. In particular x^n-1 is regular and hence by (theorem 3.2.8) – (Hensels' Lemma) x^n-1 is the product of basic irreducible polynomials and such polynomials are primary (by theorem 3.2.10). Hence by theorem 3.2.11 we immediately get the following.

3.2.12 Corollary

If x^n-1 $= f_1 f_2 ..... f_r$, where the f_i are basic irreducible and pairwise coprime, then this factorization is unique.

Proof: Follows from Theorem 3.2.11.

3.3 Ideals of the ring $Z_{p^m}[x] / \langle f(x) \rangle$

In this section we discuss the structure of the ideals of the ring $Z_{p^m}[x] / \langle f(x) \rangle$ for a basic irreducible polynomial f in Z_{p^m}.

We start by the following theorem which will play a crucial role in the characterization of generators for cyclic Z_{p^m} – codes.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.3.1 Theorem [7]

If $f(x) \in Z_{p^m}[x]$ is a basic irreducible polynomial then the ideals of $Z_{p^m}[x] / \langle f(x) \rangle$ are precisely (0), (1 + ($f(x)$), (p + ($f(x)$), ..., ($p^{m-1} + (f(x))$.

Proof:

Let I be a nonzero ideal of $Z_{p^m}[x] / \langle f(x) \rangle$. Let $g(x) + (f(x))$ be a nonzero element of I. By hypothesis, μf is an irreducible polynomial and, hence, $g.c.d\,(\mu f(x), \mu g(x)) = 1$ or $\mu f(x)$. If $g.c.d\,(\mu f(x)), \mu g(x)) = 1$ then, by (Theorem 3.2.4), f and g are coprime. Hence, there exist $u(x)$ and $v(x)$ such that: $f(x)u(x) + g(x)v(x) = 1$. But then $(g(x) + f(x))$ $(v(x) + f(x)) = 1 + (f(x))$. Therefore $g(x) + (f(x))$ is invertible. Consequently, $I = Z_{p^m}[x] / \langle f(x) \rangle$. On the other hand, if $g.c.d\,(\mu f(x), \mu g(x)) = \mu f(x)$ then, there exist $u(x), v(x) \in Z_{p^m}[x]$ such that $g(x) = f(x)u(x) + p^k v(x)$, where $g.c.d\,(\mu f(x), \mu v(x)) = 1$ and k is some positive integer less than m. Thus $g(x) + f(x) \in (p^k + (f(x)))$.

Hence, there exists $1 \leq l < m$ such that $I \subset (p^l + (f(x)))$. Let k_0 be the largest positive integer l less than m such that $I \subset (p^l + (f(x)))$. In particular, there exist a nonzero element $h(x) + f(x)$ in I such that $h(x) = f(x)u(x) + p^{k0} r(x)$ and $g.c.d\,(\mu f(x), \mu r(x)) = 1$. Thus, $p^{k0} r(x) + (f(x)) \in I$ and $g.c.d\,(\mu f(x), \mu r(x)) = 1$. But then by theorem 3.2.4, f,

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

r, are coprime. Hence, there exist a(x), b(x) $\in Z_{p^m}[x]$ such that r(x)a(x) + $f(x)$b(x) = 1. Thus, $p^{k0} + (f(x)) = (p^{k0} r(x)) + (f(x))\ (a(x)) + (f(x)) \in I$. Consequently, $I = (p^{k0} + (f(x))$. And this concludes the proof of the theorem.

3.3.2 Corollary [14]

If $f(x)$ is in $Z_4[x]$ and is basic irreducible, then the only ideals of $Z_4[x] / f(x)$ are (0), (1), and (2).

Proof:

The proof follows immediately by the previous theorem with $p = 2$, $m = 2$.

Now we state the following theorem to use it in proving the next theorem.

3.3.3 Theorem (Chinese Remainder Theorem) [6]

Let $A_1, \ldots, A_n$ be ideals in a ring $\Re$, such that $\Re^2 + A_i = \Re$ for all i, and $A_i + A_j = \Re$ for all $i \neq j$. If $b_1, \ldots, b_n \in \Re$, then there exists $b \in \Re$ such that $b \equiv b_i \ (mod\ A_i)$ $(i = 1, 2, \ldots, n)$. Furthermore, b is uniquely determined up to congruence modulo the ideal $A_1 \cap A_2 \cap \ldots \cap A_n$.

3.3.4 Remark [1]

In the last theorem, if $\Re$ has an identity, then $\Re^2 = \Re$, so $\Re^2 + A = \Re$ for every ideal A of $\Re$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.3.5 Theorem [7]

Let p be a prime such that p does not divide n. Let x^n-1 = $f_1 f_2 \ldots f_r$ be the representation of x^n-1 as a product of basic irreducible pairwise – coprime polynomials in $Z_{p^m}[x]$. Then any ideal in $\Re_n$ is a sum of ideals of the type $(p^j \hat{f}_i + (x^n - 1))$, where $0 \le j \le m\text{-}1$, $1 \le i \le r$. And for $1 \le i \le r, \hat{f}_i = {(x^n - 1)}/{f_i} = \prod_{j \ne i} f_j$.

Proof:

Since the fi's are pairwise–coprime, we have $(x^n\text{-}1) = (f_1) \cap (f_2) \cap \ldots . \cap (f_r)$. And for $1 \le i, j \le r, i \ne j$, $Z_{p^m}[x] = (f_i) + (f_j)$.

Thus by (theorem 3.3.3), Chinese Remainder Theorem,

$$\Re_n = \frac{Z_{p^m}[x]}{\bigcap_{i=1}^{r} (f_i)} \cong \oplus \sum_{i=1}^{r} \frac{Z_{p^m}[x]}{(f_i)}$$

Consequently, If I is an ideal of $\Re_n$ then $I = \oplus \sum I_i$, where I_i is an ideal of the ring $Z_{p^m}[x]/(f_i)$. By (theorem 3.3.1), for each i, $1 \le i \le r$, $I_i = (0)$. Or $(p^k + (f_i))$ for some k, $0 \le k \le m\text{-}1$. But then I_i will correspond to $(p^k \hat{f}_i + (x^n - 1))$ in $\Re_n$. Hence, I is a sum of ideals of the type $(p^j \hat{f}_i + (x^n - 1))$.

3.3.6 Corollary [14]

Let $x^n\text{-}1 = f_1 f_2 \ldots . f_r$ be a product of basic irreducible and pair-wise co-prime polynomials for odd n, and let $\hat{f}_i$ denote the product

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

of all f_j except f_i. Then any ideal in the ring $\Re_n$ is a sum of some $(\hat{f}_i)$ and $(2\hat{f}_i)$.

Now we'll state the following theorem, which will be used in dual codes.

3.3.7 Theorem [11]

Let $a(x) = a_0 + a_1x + ... + a_{n-1}\, x^{n-1}$, and $b(x) = b_0 + b_1x + ... + b_{n-1}\, x^{n-1}$

Then $a(x)\ b(x) = 0$ in $\Re_n$ if and only if the vector $(a_0, a_1,.....,a_{n-1})$ is orthogonal to the vector $(b_{n-1}, b_{n-},....,b_0)$ and all its cyclic shifts.

Proof: See chapter II.

3.3.8 Theorem [7]

The number of cyclic Z_{p^m}-codes of length n is $(m + 1)^r$, where r is the number of factors in a factorization of $x^n - 1$ as a product of basic irreducible pairwise–coprime polynomials.

Proof:

The proof follows immediately from theorem (3.3.5). Recall that a code over Z_{p^m} is cyclic if and only if it is an ideal in the ring $\Re_n = Z_{p^m}[x] / (x^n - 1)$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3.3.9 Corollary [14]

The number of Z_4 cyclic codes of length n is 3^r, where r is the number of basic irreducible polynomial factors in $x^n - 1$.

Proof: Follows from Theorem 3.3.8 with $m = 2$.

3.4 Generator polynomials

From this point on, in order to simplify the notation when dealing with the elements of the ring $\Re_n = Z_{p^m}[x]/(x^n - 1)$, we will use the polynomials in $Z_{p^m}[x]$ of degree less than n to represent their corresponding cosets in $\Re_n$.

3.4.1 Theorem [7]

Suppose p is a prime not dividing n, and C is a cyclic Z_{p^m} code. Then there exists a collection of pairwise-coprime polynomials F_0, F_1, ..., F_m (possibly equal to 1) such that $F_0F_1....F_m = x^n - 1$ and C is generated by $\{\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m\}$; i.e., $C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m)$.

The polynomials $F_0, F_1, ..., F_m$ are unique in the sense that if $C = (\hat{H}_1, p\hat{H}_2, ..., p^{m-1}\hat{H}_m)$, where $H_0, H_1, ... H_m = x^n - 1$ then for $0 \le i \le m$, F_i is an associate of H_i. In particular, if we require the F_i's to be monic then the representation is unique. Moreover, $|C| = p^k$, where $k = \sum_{i=0}^{m-1}(m-i)\deg F_{i+1}$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Proof:

Let $x^n - 1 = f_1 f_2 \ldots f_r$, where $f_1, f_2, \ldots, f_r$ are unique basic irreducible pairwise–coprime polynomials. $f_1, f_2, \ldots, f_r$ may be chosen to be monic. For each i, $1 \le i \le r$, let $\hat{f}_i$ denote the product of all f_i's different from f_i. Then, from (theorem 3.3.5) C is a sum of ideals of the type $(p^j \hat{f}_i)$. By reordering, if necessary, we can assume that C is the sum of:

$$(\hat{f}_{k_1+1}),(\hat{f}_{k_1+2}),\ldots,(\hat{f}_{k_1+k_2});(p\hat{f}_{k_1+k_2+1}),\ldots,(p\hat{f}_{k_1+k_2+k_3});\ldots;(p^{m-1}\hat{f}_{k_1+k_2+\ldots+k_{m+1}}),\ldots,(p^{m-1}\hat{f}_r)$$

Let $k_0 = 0$ and, for $0 \le i \le m$,

$$F_i = \begin{cases} 1 & \text{if } k_{i+1} = 0 \\ f_{k_0+k_1+k_2+\ldots+k_{i+1}} \ldots f_{k_0+k_1+k_2+\ldots+k_{i+1}} & \text{if } k_{i+1} \neq 0 \end{cases}$$

So $C = (\hat{F}_1, p\hat{F}_2, \ldots\ldots\ldots, p^{m-1}\hat{F}_m)$. Observe that if for $0 \le j \le m$,

$A_j = \{i \mid 1 \le i \le r, p^{m-j}\hat{f}_i \in C, p^{m-j-1}\hat{f}_i \notin C\}$. Then $F_j = \Pi_{i \in A_j} f_i$.

The uniqueness of the F_i's follows from this observation and the uniqueness of the f_i's. If each $F_i \neq 1$ $(1 \le i \le m)$ then they are pairwise-coprime and thus $C = (\hat{F}_1) \oplus (p\hat{F}_2) \oplus \ldots\ldots \oplus (p^{m-1}\hat{F}_m)$. Therefore,

$$|C| = |(\hat{F}_1)||(p\hat{F}_2)|\ldots\ldots\ldots|(p^{m-1}\hat{F}_m)|$$

$$= p^{m(n-\deg \hat{F}_1)} p^{(m-1)(n-\deg \hat{F}_2)} \ldots\ldots\ldots p^{(m-\deg \hat{F}_m)} = p^k,$$

where $k = \sum_{i=0}^{m-1} (m-i)\deg F_{i+1}$ as desired. If $F_i = 1$ for some i, a slight modification will yield the result and the formula for $|C|$ still holds.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

And hence the proof is complete.

3.4.2 Remark

Some of the generators above may be equal to zero. Namely, if for some k, $1 \leq k \leq m$, $f_k = 1$, then $\hat{F}_k = F_0 F_1 \ldots\ldots F_{k-1} F_k \ldots\ldots F_m = 0(\mathrm{mod}(x^n - 1))$

3.4.3 Corollary [14]

Suppose C is a Z_4 cyclic code of odd length n. Then there are unique monic polynomials f, g and h such that $C = (fh, 2fhg)$, where $fgh = x^n\text{-}1$, and $|C| = 4^{n\text{-}degf\text{-}degh}\, 2^{n\text{-}degf\text{-}degg}$.

When $h = 1$, $C = (f)$ and $|C| = 4^{n\text{-}degf}$.

When $g = 1$, $C = (2f)$ and $|C| = 2^{n\text{-}degf}$.

Proof: Follows immediately from the previous theorem.

3.4.4 Theorem [7]

Suppose p is a prime not dividing n and C is a cyclic Z_{p^m} code. Then there exist polynomials $f_0, f_1, \ldots\ldots, f_{m\text{-}1}$ such that:

$f_{m\text{-}1} \mid f_{m\text{-}2} \mid \ldots\ldots\ldots \mid f_0 \mid x^n - 1$. And $C = (f_0, pf_1, p^2 f_2, \ldots\ldots, p^{m\text{-}1} f_{m\text{-}1})$.

Proof:

By Theorem 3.4.1, $C = (\hat{F}_1, p\hat{F}_2, \ldots\ldots\ldots, p^{m-1}\hat{F}_m)$. For $0 \leq i \leq m - 2$, let $f_i = F_0 F_{i+2} \ldots\ldots F_m$ and $1 f_{m\text{-}1} = F_0$. Then $f_{m\text{-}1} \mid f_{m\text{-}2} \mid \ldots\ldots \mid f_0 \mid x^n\text{-}1$.

Also for all I, $0 \leq i \leq m\text{-}1$, $p^i \hat{F}_{i+1} = p^i F_0 F_1 \ldots\ldots F_i F_{i+2} \ldots\ldots F_m = p^i f_i F_1 F_2 \ldots\ldots F_i$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Hence $C \subset (F_0, pf_1, \ldots, p^{m-1}f_{m-1})$. To prove the reverse inclusion first observe that $f_0 \in C$. Since F_1 and F_2 are coprime, there exist polynomials $a(x), b(x) \in Z_{p^m}[x]$ such that $1 = a(x)F_1(x) + b(x)F_2(x)$. Thus $pF_1 - pF_0F_3\ldots F_m = pa(x)F_0F_1F_3\ldots F_m + pb(x)f_0 = pa(x)\hat{F}_2 + pb(x)f_0 \in C$. Proceeding like this we get $p^i f_i \in C$ for all i, $0 \le i \le m-1$. Thus $C = (f_0, pf_1, \ldots, p^{m-1}f_{m-1})$.

3.5 Dual and self-dual Z_{p^m} cyclic codes

Recall that, for a Z_{p^m} code C, a code is called self-dual if it is its own dual. (*i.e.* $C = C^{\perp}$).

Before we go on to produce generators for the dual codes, we need to state the following well-known Lemma.

3.5.1 Lemma [7]

The number of elements in any nonzero linear code C over Z_{p^m} is of the form p^k. Furthermore, the dual code $C^{\perp}$ has p^l codewords where $k + l = mn$.

3.5.2 Theorem [7]

Suppose p is a prime not dividing n and $C = (\hat{F}_1, p\hat{F}_2, \ldots, p^{m-1}\hat{F}_m)$, where $F_0F_1\ldots\ldots F_m = x^n - 1$. Then $C^{\perp} = (\hat{F}_0^*, p\hat{F}_m^*, p^2\hat{F}_{m-1}^*, \ldots, p^{m-1}\hat{F}_2^*)$

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Proof:

We assume that $F_i \neq 1$ for all i, $1 \leq i \leq m$. The case when some $F_i = 1$ can be dealt with similarly. Let $C_1 = (\hat{F}_0^*, p\hat{F}_m^*, p^2\hat{F}_{m-1}^*, \ldots, p^{m-1}\hat{F}_2^*)$. First observe that $0 \leq i, j \leq m-1$. $(p^i\hat{F}_{i+1})(p^j\hat{F}_{m-j+1}^*)^*$ is divisible by $x^n - 1$ if $i + 1 \neq m-j+1$, and is divisible by p^m if $i + 1 = m-j+1$.

In any case $(p^i\hat{F}_{i+1})(p^j\hat{F}_{m-j+1}^*)^* \equiv 0 (\mathrm{mod}\, x^n - 1)$. Thus $C_1 \subset C^{\perp}$. Also, $|C_1| = p^{m \deg F_0^*} p^{(m-1)\deg F_m^*} \ldots\ldots p^{\deg F_2^*} = p^t$, where $t = \sum_{i=1}^{m} i \deg F_{i+1}$, with $F_{m+1} = F_0$. On the other hand by lemma 3.5.1, $|C^{\perp}| = p^l$, where $l + k = n$. By theorem 3.4.1, $k = \sum_{i=0}^{m-1} (m-i) \deg F_{i+1}$. It follows that $l = \sum_{i=1}^{m} i \deg F_{i+1} = t$ (with $F_{m+1}=F_0$). Hence $C^{\perp} = C_1$, and the proof is complete.

3.5.3 Theorem [12]

Let $C = (fh, 2fg)$ be a Z_4 cyclic code of odd length n, where f, g and h are monic polynomials such that $fgh = x^n - 1$. And $|C| = 4^{degg} 2^{degh}$. Then, $C^{\perp} = (g^*h^*, 2g^*f^*)$.

If $h = 1$, then $C = (f)$ and $C^{\perp} = (g^*)$.

If $g = 1$, then $C = (2f)$ and $C^{\perp} = (h^*, 2f^*)$

Proof:

By Theorem 3.3.7, we know that $(g^*h^*) \subseteq (fh, 2fg)^{\perp}$. And similarly $(2g^*f^*) \subseteq (fh, 2fg)^{\perp}$. Therefore $(g^*h^*, 2g^*f^*) \subseteq (fh, 2fg)^{\perp}$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Since $|(g^*h^*, 2g^*f^*)| = 4^{n-deg(g)-deg(h)}2^{n-deg(g)-deg(f)} = |(fh, 2fg)^{\perp}|$.

So we have: $(g^*h^*, 2g^*f^*) = (fh, 2fg)^{\perp}$.

In the next theorem we characterize self-dual Z_{p^m}–codes.

3.5.4 Theorem [7]

Suppose $C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m)$, where $F_0F_1.....F_m = x^n - 1$ and p does not divide n. Then C is self-dual if and only if for $0 \le i, j \le m$ whenever $i + j \equiv 1 \ (mod\ m+1)$, F_i is an associate of F_j^*.

Proof:

If for $0 \le i, j \le m$, $i + j \equiv 1 (mod\ m+1)$, F_i is an associate of F_j^* then obviously C is self-dual. To prove the other direction, let $G_i = F_j^*$ whenever $0 \le i, j \le m$ are such that $i + j \equiv 1 (mod\ m+1)$.

Then we have $G_0G_1.....G_m = x^n\text{-}1 = F_0F_1....F_m$ and since $C = C^{\perp}$, we have from uniqueness in theorem 3.4.1, that for all i, $0 \le i \le m$,

F_i is an associate of G_i. In other words F_i is an associate of F_j^* whenever $0 \le j \le m$ are such that $i + j \equiv 1 (mod\ m+1)$.

3.5.5 Corollary [13]

Let C be a cyclic code over Z_4, $C = (fh, 2fg)$ where $fgh = x^n - 1$, n odd.

Then C is self-dual if and only if $F = ug^*$ and $h = uh^*$, where u is a unit and g^* is the reciprocal of g.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

The following theorem provides a criterion that determines the existence of nontrivial self-dual cyclic Z_{p^m} codes.

3.5.6 Theorem [7]

If p is a prime that does not divide n and m is even, then nontrivial self-dual cyclic Z_{p^m}-codes exist if and only if there exists a basic irreducible polynomial $f \in Z_{p^m}[x]$ such that $f \mid x^n - 1$ and f is not an associate of f^*.

Proof:

Suppose $C = (\hat{F}_1, p\hat{F}_2, \ldots\ldots, p^{m-1}\hat{F}_m)$, where $F_0F_1\ldots\ldots F_m = x^n - 1$.

If, for every $f \in Z_{p^m}[x]$ such that $f \mid x^n - 1$, f is an associate of f^* then, for $0 \le i \le m$, F_i is an associate of F_i^*. Now if C is self-dual, then whenever $0 \le i, j \le m$ and $i + j \equiv 1 (mod\ m+1)$, F_i is an associate of F_j^*, and hence, of F_j. Thus, since $x^n - 1$ has no repeated roots,

$F_i \neq 1$ only if $i = \frac{m}{2} + 1$. Consequently, $F_{\frac{m}{2}+1} = x^n - 1$ and $C = (p^{\frac{m}{2}})$, is the trivial self-dual cyclic Z_{p^m} – code.

Conversely, if there exists a basic irreducible polynomial $f \in Z_{p^m}[x]$, such that $f \mid x^n - 1$ and f is not an associate of f^* then, there exists $h \in Z_{p^m}[x]$ such that $x^n - 1 = ff^*h$. Writing $m = 2k$, then the cyclic code $(p^{k-1}f^*h, p^kff^*, p^{k+1}fh)$ is not trivial and self-dual.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Proof: Follows from the previous theorem.

3.5.7 Corollary

Non-trivial cyclic, self-dual codes of length n exist if and only if $-1 \neq 2^i \pmod{n}$ for any i.

3.6 Idempotents

Recall that $e(x) \in \mathfrak{R}_n$ is called idempotent if $[e(x)]^2 = e(x)$, equivalently, as polynomials, $[e(x)]^2 \equiv e(x) \pmod{(x^n - 1)}$.

3.6.1 Example

$e(x) = x + x^2 + x^4$ is an idempotent element of $Z_2[x]/(x^7 - 1)$, but it is not idempotent element of $Z_{2^m}[x]/(x^7 - 1)$ when $m \geq 2$.

3.6.2 Theorem [7]

1. Suppose p is a prime not dividing n and C is an ideal of $\mathfrak{R}_n$. If C is generated by a divisor f of $x^n - 1$ then C has an idempotent generator e. Furthermore, whenever $0 \leq k \leq m-1$, then $(p^k f) = (p^k e)$.

2. Suppose p is a prime not dividing n and f is adivisor of $x^n - 1$. Then for each k such that $0 \leq k \leq m - 1$, there exist an idempotent $e_k \in Z_{p^m}\, k[x]/(x^n - 1)$ such that $(p^k f) = (p^k e_k)$.

Indeed, if $\mu_k : Z_{p^m}[x] \rightarrow Z_{p^{m-k}}[x]$ is the ring homomorphism that maps $a + (p^m)$ to $a + (p^{m-k})$ and x to x, then e_k is the generator of $(\mu_k f)$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

3. If p is a prime not dividing n, f is adivisor of $x^n - 1$ and $e(x)$ is the binary idempotent generator of $(\mu f) \leq Z_2[x]/(x^n - 1)$, then $(2^{m-1}f) = (2^{m-1}e)$.

Proof:

1. Since p does not divide n and f divides $x^n - 1$, there exists $g \in \Re_n^{(m)}$ such that $fg = x^n - 1$ and f and g are coprime. Thus, there exist $a(x)$, $b(x) \in Z_{p^m}[x]$ such that $af + bg = 1$. Let $e \in \Re_n^{(m)}$ be congruent to $f \pmod{x^n - 1}$, then $e \equiv 1 - bg$. Thus, $e^2 \equiv e(1 - bg) = e - ebg = e - abfg \equiv e$. It follows that $fe = f - fbg \equiv f \pmod{x^n - 1}$. Thus e is an idempotent and $(f) = (e)$. Clearly, this also implies that, for $1 \leq k \leq m-1$, $(p^k f) = (p^k e)$.

2. For $0 \leq k \leq m-1$, Let $\mu_k : Z_{p^m} \rightarrow Z_{p^{m-k}}[x]$ be the ring homomorphism that maps $a + (p^m)$ to $a + (p^{m-k})$ and x to x.

Since $f \mid x^n - 1$ in $Z_{p^m}[x]$, $\mu_k f$ divides $x^n - 1$ in $Z_{p^{m-k}}[x]$.

By (1), there exists $ek \in Z_{p^{m-k}}[x]/(x^n - 1)$, such that $(\mu_k f) = (ek)$.

Since $p^k f = p^k \mu_k f$, it follows that $(p^k f) = (p^k e_k)$.

3. Follows from (2).

3.6.3 Corollary [14]

Let C be Z_4 cyclic code of odd length n.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

1. If $C = (f)$, where $fg = x^n - 1$ for some g, then C has an idempotent generator in Z_4.

2. If $C = (2f)$ and f divides $x^n - 1$, then $C = (2e)$, where e is a binary idempotent generator of (μ_f).

3. If $C = (fh, 2fg)$, where $fgh = x^n - 1$, then $C = (e, 2v)$, where e is an idempotent in Z_4, v is an idempotent in Z_2.

Proof: Follows from theorem 3.6.2.

Recall that If C_1 and C_2 are cyclic Z_{p^m}-codes with idempotent generators e_1 and e_2 respectively, then e_1e_2 and $e_1 + e_2 - e_1e_2$ are idempotent generators of $C_1 \cap C_2$ and C_2, respectively. (Theorem 2.6.7) If $C_1 \cap C_2 = (0)$ then $e_1 + e_2$ is an idempotent generator of $C_1 \oplus C_2$. Using this fact with theorem 3.6.2, we get the following corollary.

3.6.4 Corollary [7]

Suppose $C = (\hat{F}_1, p\hat{F}_2, ..., p^{m-1}\hat{F}_m)$, where F_0, F_1, ..., F_m are pairwise – coprime polynomials in $Z_{p^m}[x]$ such that $F_0, F_1, ..., F_m = x^n - 1$. Then $C = (e_0, pe_1, ..., p^{m-1}e_{m-1})$, where for each k such that $0 \le k \le m-1$, e_k is an idempotent in $Z_{p^{m-k}}[x]/(x^n - 1)$.

3.6.5 Lemma [8]

If $e(x)$ is the idempotent generator of a cyclic Z_{p^m}-code, then $1 - e(x^{-1})$ is the idempotent generator f $C^{\perp}$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

Proof: See chapter II.

3.6.6 Example (cyclic Z_9-codes of length 4).

In $Z_9[x]$, $x^4 - 1 = (x - 8)(x + 8)(x^2 + 1) = f_0 f_1 f_2$,

where $f_0 = x - 8$, $f_1 = x + 8$, $f_2 = x^2 + 1$. Observe that f_0, f_1, f_2 are basic irreducible, pair-wise-coprime and $f_0^* = f_0, f_1^* = -f_1, f_2^* = f_2$.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

And now we list all nontrivial cyclic Z_9- codes of length 4 along with their duals and length.

Generator of the code	Generator of the dual code	Order of the code
3	3	3^4
f_0	f_1f_2	9^3
f_1	f_0f_2	9^3
f_2	f_0f_1	9^2
$3f_0$	$(f_1,f_2,3f_0)$	3^3
$3f_1$	$(f_0f_2,3f_1)$	3^3
$3f_2$	$(f_0f_1,3f_2)$	3^2
f_0f_1	f_2	9^2
f_1f_2	f_0	9
f_0f_2	f_1	9
$3f_0f_1$	$(f_2,3f_0f_1)$	3^2
$3f_1f_2$	$(f_0,3f_1f_2)$	3
$3f_0f_2$	$(f_1,3f_0f_2)$	3
$(f_1f_2,3f_0)$	$3f_0$	9.3^3
$(f_0f_2,3f_1)$	$3f_1$	9.3^3
$(f_0f_1,3f_2)$	$3f_2$	$9^2.3^2$
$(f_2,3f_0f_1)$	$3f_0f_1$	$9^2.3^2$
$(f_0,3f_0f_2)$	$3f_0f_2$	$9^3.3$
$(f_0,3f_1f_2)$	$3f_1f_2$	$9^3.3$
$(f_0f_2,3f_0f_1)$	$(f_1f_2,3f_0f_1)$	9.3^2
$(f_0f_1,3f_0f_2)$	$(f_1f_2,3f_0f_2)$	$9^2.3$
$(f_1f_2,3f_1f_0)$	$(f_0f_2,3f_0f_1)$	9.3^2
$(f_1f_0,3f_1f_2)$	$(f_0f_2,3f_1f_2)$	$9^2.3$
$(f_1f_2,3f_0f_2)$	$(f_0f_1,3f_0f_2)$	9.3
$(f_2f_0,3f_1f_2)$	$(f_0f_1,3f_2f_1)$	9.3

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

References:

1. D. M. Burton, Elementary Number theory, Brown, Oxford, England, 1989.
2. J. H. Conway, and N. J. Sloane, Self-dual Codes over the integers modulo 4, J. Combin. Theory Ser. AG_2 (1993), 30-45.
3. Eugene, Spiegel, Codes over Z_m, Inform. Control 35 (1977), 48-51.
4. Eugene, Spiegel, Codes over Z_m, Revisited, Inform. and Control 37(1978), 100-104.
5. D. G. Hoffman, Coding Theory, 1990, Marcel Dekker, Inc., 1990.
6. T. W. Hungerford, Algebra, springer-verlag., 1974.
7. P. Kanwar, and S. R. López-Permouth, Cyclic Codes over the integers Modulo p^m, Finite Fields and their applications 3(1997), 334-352.
8. F. J. Macwilliams, and N. J. Sloane, The theory of Error – correcting codes, North Holland, 1998.
9. B. R. McDonald, Finite rings with identify, Dekker, NewYork, 1974.
10. P. B., Jain S. K., Basic Abstract algebra, Cambridge University press, 1996.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

11. V. Pless, Introduction to the theory of error correcting codes, Wiley, NewYork, 1989.

12. V. Pless, and Z. Qian, Cyclic codes and quadratic codes over Z_4, IEEE Trans. Inform. Theory 42(1996), 1594-1600.

13. V. Pless, P. Solé and Z. Qian, Cyclic self-dual Z_4-codes, Finite Fields Appl. 3(1997), 48-69.

14. Z. Qian, Cyclic codes over Z_4, ph.d. dissertation, University of Illinois at Chicago, 1996.

15. S. Roman, Coding and Information theory, 1968, springer-verlag-, 1968.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit

الخـــلاصـــة

تم في هذه الرسالة دراسة تعاريف ومفاهيم أساسية في نظرية الشيفرة، منها: خصائص الشيفرة الخطية، واكتشاف وتصحيح الخطأ في الشيفرة، ومفاهيم جبرية أخرى. كما تم دراسة الشيفرات الدورية وخصائصها مثل مولداتها كثيرات الحدود و (Their idempotents). وتمت مناقشة كيفية إرسال الشيفرة الدورية وتصحيحها بعد استقبالها. ثم عرضت بعض أنواع الشيفرات الدورية مثل شيفرات هامنغ (Hamming Codes).

كما نوقشت، بشكل تفصيلي، خصائص الشيفرات المعرفة على الحلقة Z_{p^m}، بما في ذلك مولداتها ونظائرها (Their generators, their duals) ونظائرها الذاتية، وكيفية إيجاد كل منها.

All Rights Reserved - Library of University of Jordan - Center of Thesis Deposit