A STUDY OF

NEGACYCLIC CODES

by

CHAU VAN CHINH

Submitted to the Department of Electrical Engineering in partial fulfilment of the requirements for the degree of Master of Applied Science.

Department of Electrical Engineering,
Faculty of Science and Engineering,
University of Ottawa.
Ottawa, Ontario.

February 1974.

ACKNOWLEDGEMENTS

The author wishes to thank his supervisor, Professor S. G. S. Shiva, for his help in research leading to this thesis.

The author would like to thank also the graduate students in the Department who contributed useful thoughts through discussion.

Finally, thanks are also due to the National Research Council of Canada, The Department of Communications and the University of Ottawa for financial assistance.

ABSTRACT

This thesis deals with negacyclic codes. These codes, due to Berlekamp, are similar to the more well-known cyclic codes and can be implemented almost as easily as the latter codes. In fact, as will be shown in the thesis, many of the techniques developed for cyclic codes can be easily extended to negacyclic codes. In particular the topics considered are (i) the decoding of negacyclic codes with small error-correcting capability, (ii) permutation decoding and (iii) synchronization. Also included is a list of generator polynomials for both primitive and non-primitive negacyclic codes.

TABLE OF CONTENTS.

INTRODUCTION

Because of rapid advances in technology, the idea of using error-correcting codes instead of merely error-detecting codes in processes like data-transmission, data-storage and telemetry is becoming more and more attractive by way of speed, cost and size [1, 2]. If the channel is one-way so that a request-for-repeat cannot be made, after detecting an error, from the receiver to the transmitter, then the use of error-correcting codes (Forward Error Correction) is the only solution [3].

Error-correcting codes can be classified in many ways. One such way would be to classify them as being cyclic or non-cyclic. The class of cyclic codes has received greater attention than that of non-cyclic codes. This is probably because cyclic codes are simpler from the point of view implementation.

In discussing and developing the random-error-correcting capability of codes, the idea of distance is basic. The metric invariably used to express the distance is the Hamming metric, the one notable exception being the Lee metric.

While the Hamming weight [7] is well suited to orthogonal modulation schemes, the Lee metric is well suited to phase-modulation schemes.

One class of codes which can correct all error patterns of sufficiently low Lee weight [7] is that of Negacyclic Codes [6,9] invented by Berlekamp.

In this thesis we discuss negacyclic codes. In Chapter I the necessary algebraic concepts will be introduced. In Chapter II will be discussed the various properties of negacyclic codes. We show how the techniques developed for cyclic codes can be used for negacyclic codes with little or no modification. In particular we consider the problems of generation of negacyclic codes, general decoding, permutation decoding, majority-logic decoding and synchronization. The thesis will be concluded with remarks about what can conceivably be done further in regard to negacyclic codes.

CHAPTER I

NECESSARY ALGEBRAIC CONCEPTS

In this chapter we introduce briefly the algebraic facts necessary for the development of the thesis . For details reference may be made to any standard book on algebra or coding theory [4 , 11].

A GROUP G is a set of elements satisfying the following 4 conditions :

i. For any two elements g_1 and g_2 in G , $g_1 \odot g_2$ belongs to G .

ii. For any three elements g_1 , g_2 and g_3 in G, $(g_1 \odot g_2) \odot g_3 = g_1 \odot (g_2 \odot g_3)$.

iii. There is an identity element g_0 of G such that $g_1 \odot g_0 = g_0 \odot g_1 = g_1$.

iv. Every element g_1 has an inverse g_1^{-1} belonging to G such that $g_1 \odot g_1^{-1} = g_0$.

Here $\odot$ indicates the one operation defined on G .

An ABELIAN GROUP is a group in which $g_1 \odot g_2 = g_2 \odot g_1$ for every two elements g_1 and g_2 of the group.

A RING R, on which two operations are defined, is a set of elements satisfying the following 4 conditions:

i. R is an abelian group under addition.

ii. For any two elements r_1 and r_2 of R, $r_1 r_2$ (product) belongs to R.

iii. For any three elements r_1, r_2 and r_3 of R, $r_1(r_2 r_3) = (r_1 r_2) r_3$.

iv. For any three elements r_1, r_2 and r_3 of R, $r_1(r_2 + r_3) = r_1 r_2 + r_1 r_3$.

A COMMUTATIVE RING is a ring in which, for every two elements r_1 and r_2 of the ring, $r_1 r_2 = r_2 r_1$.

A FIELD F is a commutative ring with a multiplicative identity, every non-zero element of F having a multiplicative inverse.

An n-TUPLE is a sequence of n digits.

A p-ary n-tuple is a sequence of n digits picked from a set of p symbols.

In particular we are interested in what are usually

termed as Galois Fields . By GF (p^r) we mean a Galois field of p^r elements .

What we need in this thesis are (p^r) , where p is prime . Hereafter we shall , therefore , take p to be prime .

In this thesis we shall take an n-Tuple over GF (p) to mean a sequence $a_0 a_1 \ldots a_{n-1}$, where $a_i \in$ GF (p) .

Associated with such a sequence is a POLYNOMIAL

$$A(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} .$$

The polynomial A(x) is said to be IRREDUCIBLE over GF(p) if it can not be factored further .

A polynomial A(x) over GF (p) is said to have an EXPONENT e if A(x) divides $x^e - 1$ and not $x^{e'} - 1$ for any $e' < e$, all operations being over GF (p).

With $n = p^r - 1$, every irreducible factor of $x^n - 1$ over GF (p) has degree r or less .

The roots of $x^n - 1$ can be expressed in the form $\alpha , \alpha^2 , \ldots , \alpha^{n-1} , \alpha^n = 1$, where α is said to be a PRIMITIVE root . The set $\{0 , 1 , \alpha , \alpha^2 , \ldots , \alpha^{n-1}\}$ is a GF (p^r) .

The procedure for constructing such a field is as follows :

First we choose a polynomial $P_1(x)$ which is irreducible over GF(p), divides $x^n - 1$ and has exponent n. (Such a polynomial is called a PRIMITIVE POLYNOMIAL). This polynomial will have degree r. If

$$P_1(x) = \phi_0 + \phi_1 x + \phi_2 x^2 + \ldots\ldots + \phi_r x^r$$

for $\phi_0 \neq 0$ and $\phi_r \neq 0$, and α is a root of $P_1(x)$, then

$$P_1(\alpha) = \phi_0 + \phi_1 \alpha + \phi_2 \alpha^2 + \ldots\ldots + \phi_r \alpha^r = 0,$$

so that

$$\phi_r \alpha^r = -(\phi_0 + \phi_1 \alpha + \phi_2 \alpha^2 + \ldots\ldots + \phi_{r-1} \alpha^{r-1}).$$

Using this relation (logic) every α^i can be expressed as a linear combination of the basis vectors $1, \alpha, \alpha^2, \ldots \alpha^{r-1}$. The set of α^i so generated, together with 0, is a GF (p^r).

To illustrate this remark, let us consider the case of p = 7 and r = 2 so that $n = p^2 - 1 = 48$. One of the factors of $x^{48} - 1$, which satisfies the properties of $P_1(x)$ is $x^2 + 3x - 2$. Taking $P_1(x) = x^2 + 3x - 2$, we have

Table I : Non-zero elements of GF(7^2) with α is a root of $x^2 + 3x - 2$.

$\alpha^0 = 1$

$\alpha^1 = \alpha$

$\alpha^2 = 2 - 3\alpha$ $\quad \{\alpha^2 + 3\alpha - 2 = 0\}$

$\alpha^3 = 1 - 3\alpha$ $\quad \{\alpha^3 = \alpha . \alpha^2 = \alpha (2 - 3\alpha) = 2\alpha - 3\alpha^2$

$= 2\alpha - 3(2 - 3\alpha) = -6 + 11\alpha$

$= 1 - 3\alpha\}$

$\alpha^4 = 1 + 3\alpha$

$\alpha^5 = -1 - \alpha$

$\alpha^6 = -2 + 2\alpha$

$\alpha^7 = -3 - \alpha$

$\alpha^8 = -2$

$\alpha^9 = -2\alpha$

$\alpha^{10} = 3 - \alpha$

$\alpha^{11} = -2 - \alpha$

$\alpha^{12} = -2 + \alpha$

$\alpha^{13} = 2 + 2\alpha$

$\alpha^{14} = -3 + 3\alpha$

$\alpha^{15} = -1 + 2\alpha$

$\alpha^{16} = -3$

$\alpha^{17} = -3\alpha$

$a^{18} = 1 + 2a$

$a^{19} = -3 + 2a$

$a^{20} = -3 - 2a$

$a^{21} = 3 + 3a$

$a^{22} = -1 + a$

$a^{23} = 2 + 3a$

$a^{24} = -1$

$a^{25} = -a$

$a^{26} = -2 + 3a$

$a^{27} = -1 + 3a$

$a^{28} = -1 - 3a$

$a^{29} = 1 + a$

$a^{30} = 2 - 2a$

$a^{31} = 3 + a$

$a^{32} = 2$

$a^{33} = 2a$

$a^{34} = -3 + a$

$a^{35} = 2 + a$

$a^{36} = 2 - a$

$a^{37} = -2 - 2a$

$a^{38} = 3 + 3a$

$a^{39} = 1 - 2a$

$$a^{40} = 3$$

$$a^{41} = 3a$$

$$a^{42} = -1 + 2a$$

$$a^{43} = 3 - 2a$$

$$a^{44} = 3 + 2a$$

$$a^{45} = -3 - 3a$$

$$a^{46} = 1 + a$$

$$a^{47} = -2 - 3a$$

$$a^{48} = 1$$

Let I be a subset of a ring R such that I is a group under addition and , for $i \in I$ and $r \in R$, ir and ri belong to I . Then I is said to be an IDEAL . If R is commutative , then , of course., ir = ri . In such a case we get a one-sided ideal as opposed to the two-sided ideal of the non-commutative ring .

A subset of a ring R is an ideal if and only if every element of the subset is a multiple of a generator element g which belongs to the subset .

The set of polynomials modulo $x^{\nu}-1$ over GF (p) form a ring . In this ring of polynomials , a subset is an ideal if and only if every polynomial of the subset is a multiple of some g(x) which belongs to the subset . It can be shown that a set V of polynomials modulo $x^{\nu}-1$ is an ideal if and only if every element V(x) of V can be expressed in the form

$$V(x) = g(x)C(x) \text{ modulo } x^{\nu}-1 ,$$

where g(x) divides $x^{\nu}-1$.

Since C(x) has a degree $< k = \nu$- degree of g(x) , there are p^k distinct possibilities for C(x) . Thus the ideal V has p^k elements . The number k is said to be the DIMENSION of V .

If a polynomial B(x) has degree $\nu-1$ or less , then xB(x) modulo $x^{\nu}-1$ is said to be a CYCLIC SHIFT of B(x) .

A set of polynomials modulo $x^{\nu}-1$ is said to be CYCLIC if , for every B(x) belonging to the set , the cyclic shift of B(x) also belongs to the set .

It can be shown that a set of polynomials modulo $x^{\nu}-1$ is cyclic if and only if it is an ideal .

In view of this fact the ideal V is a cyclic set .

Such a set is called a CYCLIC CODE in coding theory .

If $\nu = n = p^r - 1$, then V is said to be a PRIMITIVE CYCLIC CODE . If $\nu \neq n$, then the code is said to be NONPRIMITIVE .

From the discussion so far it is clear that the generator polynomial $g(x)$ of a cyclic code divides $x^n - 1$. At this point it is natural to wonder about the set of all the multiples of a polynomial which divides $x^n + 1$ instead of $x^n - 1$. This aspect will be discussed in the next chapter .

CHAPTER II

NEGACYCLIC CODES.

2-1. NEGACYCLIC CODES.

In this chapter we discuss the class of negacyclic codes. The topics considered are general decoding, permutation decoding, synchronization and majority-logic decoding.

A NEGACYCLIC CODE V of block length n over GF(p) (p is prime > 2 and n is a non-multiple of p) is the set of all multiples of a generator polynomial g(x) which divides $x^n + 1$ over GF(p). The quotient $h(x) = \frac{x^n + 1}{g(x)}$ is called the parity check polynomial.

In the discussion of negacyclic codes we require the Lee metric rather than the Hamming metric.

The LEE WEIGHT of the n-tuple $a_0 a_1 a_2 \ldots a_{n-1}$ over GF(p) is the sum of the Lee weights of a_i.

The Lee weight of $a_i = |a_i| = \pm a_i$ modulo p and

$$0 \leq |a_i| \leq \frac{p-1}{2}.$$

For EXAMPLE , the sequence

$$a_0 a_1 a_2 \ldots\ldots a_5 = 1\ 2\ -2\ 4\ 0\ -1$$

over GF(5) has the Lee weight = $|1|+|2|+|-2|+|-1|+|0|+|-1| = 7$.

(Here we have $a_3 = 4 > \frac{p-1}{2} = \frac{5-1}{2}$ which does not follow the restriction $0 \leq |a_i| \leq \frac{p-1}{2}$, we have to, therefore , convert a_3 into suitable value, such as $a_3 = 4 = -1$(modulo 5) so that $|-1| < \frac{5-1}{2}$).

By a t-RANDOM ERROR-CORRECTING negacyclic code V , we mean that V can correct any combination of t or fewer errors as long as the Lee weight of the error pattern is t or less .

For EXAMPLE , if t = 2 and p = 5 , then the error polynomial E(x) can be $a_i x^i$ with $|a_i| = 0, 1, 2$; $a_i x^i + a_j x^j$ with $|a_i| + |a_j| \leq 2$.

It is of interest to note that , since in the correction of BURST ERRORS it is the length of the burst that is involved and not the weight of the burst , negacyclic codes do not have any advantage over cyclic codes in regard to burst-error correction .

Expressing $V(x)$, an element of V, in the form

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

let us consider

$$V'(x) = -a_{n-1} + a_0x + a_1x^2 + \ldots\ldots + a_{n-2}x^{n-1},$$

where $V'(x)$ is said to be a NEGACYCLIC SHIFT of $V(x)$. We note that

$$V'(x) = xV(x) - a_{n-1}x^n - a_{n-1}$$

or

$$V'(x) = xV(x) - a_{n-1}(x^n+1).$$

Since $g(x)$ divides $V(x)$ and $x^n + 1$, it follows that $g(x)$ divides $V'(x)$. Thus we can make the following COMMENT: For every word of V, the negacyclic shift of the word also belongs to V.

This indicates why negacyclic codes are called what they are. The analogy between negacyclic codes and cyclic codes is obvious.

Analogous to the class of cyclic BCH codes we have the following known

Theorem 1: If the roots of $g(x)$ of V include $\alpha, \alpha^3, \ldots, \alpha^{2t-1}$ where $2t-1 < p$, then V is t-random-error-correcting [9].

From the theorem it is clear that the main restriction is that, for a given p, t has to be less than $\frac{p+1}{2}$. We point out that there is no such restriction in the case of BCH codes.

Since $g(x)$ divides $x^n + 1$, this also means that $g(x)$ divides $x^{2n} - 1$. Therefore $2n = p^r - 1$ or $n = \frac{p^r - 1}{2}$. In view of this we have the following COMMENT: With reference to the theorem 1, V has $n = \frac{p^r - 1}{2}$ and α is the primitive element of $GF(p^r)$.

EXAMPLE 1. If $p = 5$ and $r = 2$ and $t = 2$, then we have $GF(p^r) = GF(5^2)$ and $n = \frac{5^2 - 1}{2} = 12$. If we construct $GF(5^2)$ using $x^2 + x + 2$ which is a primitive polynomial with degree $r = 2$, then we find that $\alpha^3 = \alpha^{2t-1}$ is a root of $x^2 - 2$. Therefore

$$g(x) = (x^2 + x + 2)(x^2 - 2) = x^4 + x^3 - 2x + 1.$$

Thus this $g(x)$ generates a $(12,8)$ 2-error-correcting negacyclic code.

Since $g(x)$ divides $x^n + 1$, where $n = \frac{p^r - 1}{2}$, the knowledge of the irreducible factors of $x^n + 1$ is vital to the design of negacyclic codes.

Techniques are known to factorize polynomial completely over finite fields. However we note that such factorization over $GF(p^2)$ is comparatively simpler. Since no irreducible factor can have a degree greater than r, it follows that in the case of $r = 2$ it becomes a question of factoring $x^{2n} - 1$ into quadratics. The roots of a quadratic $x^2 + ux + v$ are given by,

$$(x + \frac{u}{2} + \frac{\sqrt{u^2 - 4v}}{2})(x + \frac{u}{2} - \frac{\sqrt{u^2 - 4v}}{2}).$$

Hence a quadratic is irreducible if $u^2 - 4v$ is not a perfect square over GF(p). Using this best it is not too laborious to factorize $x^n + 1$, $r = 2$, into quadratics.

FOR EXAMPLE, let us consider the factorization of polynomial $x^{2n} - 1 = x^{120} - 1$ into irreducible quadratics (here we take $p = 11$, $r = 2$, therefore $2n = p^2 - 1 = 120$).

First, we note that, for $u^2 - 4v$ to be a perfect square, it should have one of the values given by

$$u^2 - 4v = 0$$

$$u^2 - 4v = 1^2 = 1$$

$$u^2 - 4v = 2^2 = 4$$

$$u^2 - 4v = 3^2 = 9 = -2$$

$$u^2 - 4v = 4^2 = 16 = 5$$

$$u^2 - 4v = 5^2 = 25 = 3$$

This means that

$$u^2 = 4v + \{0,1,-2,3,4,5\},$$

or

$$4v = u^2 - \{0,1,-2,3,4,5\}$$

or

$$v = 3[u^2 - \{0,1,-2,3,4,5\}].$$

From this we get the following table:

Table 2.

u	v
0	0, -3, -5, 2, -1, -4
± 1	3, 0, -2, 5, 2, -1
± 2	1, -2, -4, 3, 0, -3
± 3	5, 2, 0, -4, 4, -1
± 4	4, 1, -1, -5, 3, 0
± 5	-2, -5, 4, 0, -3, 5

This means that if we choose any values of u and v "outside of this table", then we have an irreducible quadratic.

FOR EXAMPLE, if $u = \pm 1$, then v can be $1, -3, \pm 4, -5$.

Thus

$$(x^2 \pm x + 1),\ (x^2 \pm x - 3),\ (x^2 \pm x \pm 4),\ (x^2 \pm x - 5)$$

are all irreducible quadratic which divides $x^{120} - 1$.

Once we have all irreducible factors of $x^{120}-1$, the irreducible factors of $x^{60}+1$ are obtained by "trial-and-error" as follows:

We know that

$$x^{120}-1 = (x^{60}+1)(x^{60}-1)$$

Let

$$Y(x) = x^{60}+1,$$

$$Z(x) = x^{60}-1.$$

We get whenever it is possible, these polynomials into factors in binomials and trinomials. For instance

$$Y(x) = x^{60}+1 = (x^{20}+1)(x^{40} - x^{20}+1)$$

$$Z(x) = x^{60}-1$$

$$=(x^{30}-1)(x^{30}+1)$$

$$=(x^{10}-1)(x^{20} + x^{10} + 1)(x^{20} - x^{10}+1)(x^{10}+1)$$

We observe that $Z(x)$ can be factorized more than $Y(x)$. Therefore, the recognition of an irreducible quadratic which belongs to $x^{60}-1$ is easier than that of $x^{60}+1$. The irreducible quadratics which do not belongs to $x^{60}-1$ should belong to $x^{60}+1$. The task of factorization of $x^{n}+1$ into irreducible factors is, therefore, reduced considerably.

EXAMPLE 2. Factorization of $x^{24}+1$ ($p = 7$, $r = 2$, $n = 24$) into irreducible quadratics $x^2 + ux + v$.

We know that the quadratic $x^2 + ux + v$ is irreducible if $u^2 - 4v$ is not a perfect square. The possible cases that $u^2 - 4v$ is a perfect square are:

$$u^2 - 4v = 0$$

$$u^2 - 4v = (\pm 1)^2 = 1$$

$$u^2 - 4v = (\pm 2)^2 = 4 = -3$$

$$u^2 - 4v = (\pm 3)^2 = 9 = 2$$

Combining these equations we have a general expression:

$$v = 2[u^2 - \{0, 1, -3, 2\}]$$

Then all the cases that the values u and v give a perfect square are listed in table 3.

Table 3.

u	v
0	0, -2, -1, 3
$\pm$ 1	2, 0, 1, -2
$\pm$ 2	1, -1, 0, -3
$\pm$ 3	-3, 2, 3, 0

Excluding all values of v in table 3, a table that contains all values of v by which we can obtain irreducible quadratics are shown in table 4.

Table 4.

u	v
0	1, 2, -3
± 1	$-1, \pm 3$
± 2	$\pm 2, 3$
± 3	$\pm 1, -2$

Now let

$$x^{48}-1 = (x^{24}+1)(x^{24}-1)$$

$$= Y(x)\, Z(x).$$

Then

$$Y(x) = x^{24}+1 = (x^{8}+1)(x^{16}-x^{8}+1)$$

$$Z(x) = x^{24}-1 = (x^{12}-1)(x^{12}+1)$$

$$= (x^{6}+1)(x^{6}-1)(x^{4}+1)(x^{8}-x^{4}+1)$$

$$= (x^{2}+1)(x^{4}-x^{2}+1)(x^{2}-1)(x^{4}+x^{2}+1)(x^{4}+1)(x^{8}-x^{4}+1).$$

Referring to table 4, with $u = 0$ and $v = 1$, we have an irreducible quadratic

$$I_1(x) = x^2+1$$

We recognize that x^2+1 belongs to $Z(x)$. We reduce $Z(x)$ into $Z_1(x)$ by dividing X^2+1 from $Z(x)$, that is

$$Z_1'(x) = \frac{Z_1(x)}{x^2+1}$$

$$= (x^2-1)(x^4-x^2+1)(x^4+x^2+1)(x^4+1)(x^8-x^4+1)$$

Next, we take $u = 0$ and $v = 2$, thus the corresponding irreducible quadratic is:

$$I_2(x) = x^2+2$$

We divide this quadratic to one of the factors of $Z_1(x)$, if this factor is divisible by x^2+2, then $Z_1(x)$ is reduced to $Z_2(x)$, if this factor is indivisible by x^2+2, we try the next factor, until all the factors of $Z_1(x)$ are exhausted, we can say that x^2+2 belongs to $x^{24}+1$. In this case, we see that

$$x^2+2 \mid x^4-x^2+1$$

where x^4-x^2+1 is a factor of $Z_1(x)$, therefore

$$Z_2(x) = (x^2-1)(x^2-3)(x^4+x^2-1)(x^4+1)(x^8-x^4+1).$$

With $u = 1$ and $v = -1$, the corresponding irreducible quadratic is:

$$I_3(x) = x^2+x-1.$$

We see that x^2+x-1 can not divide any factors of $Z_2(x)$, therefore it belongs to $x^{24}+1$.

By this process, we finally obtain:

$$x^{24} + 1 = (x^2 + x - 1)(x^2 - x - 1)$$
$$(x^2 + 3x + 1)(x^2 - 3x - 1)$$
$$(x^2 + 2x - 2)(x^2 - 2x - 2)$$
$$(x^2 + 3x - 2)(x^2 - 3x - 2)$$
$$(x^2 + x + 3)(x^2 - x + 3)$$
$$(x^2 + 2x + 3)(x^2 - 2x + 3)$$

2-2. INFORMATION RATE.

With $n = p^r - 1$ and $t \leq \frac{p-1}{2}$, since every irreducible factor of $x^n + 1$ has degree r or less, the degree of the generator polynomial is $\leq rt \leq r\left(\frac{p-1}{2}\right)$. Therefore, the code has

$$\frac{k}{n} = \frac{n - (n-k)}{n} \geq \frac{n - rt}{n} \geq 1 - \frac{r\left(\frac{p-1}{2}\right)}{p^r - 1} \times 2$$

or

$$\frac{k}{n} \geq 1 - \frac{r(p-1)}{p^r - 1}$$

In terms of t, this becomes

$$\frac{k}{n} \geq 1 - \frac{r2t}{(2t+1)^r - 1}$$

taking $t = \frac{p-1}{2}$.

For the case of $r = 2$, we have

$$\frac{k}{n} \geq 1 - \frac{2}{p+1} = \frac{p-1}{p+1} .$$

Thus we have a class of negacyclic codes whose rates can be expressed in the form $\frac{p-1}{p+1}$.

EXAMPLE 3. We consider the case $p = 7$, $t = 3$.

a) If $r = 2$, then $n = \frac{p^2 - 1}{2} = 24$, the generator polynomial

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

has degree 6 (or number of parity digits = 6), the number of information digits is $k = 24 - 6 = 18$, which gives the information rate

$$\frac{k}{n} = \frac{18}{24} = {}^3/_4 .$$

b) If $r = 3$, we have $n = \frac{p^3 - 1}{2} = 171$, the generator polynomial

$$g(x) = 1 - x + 2x^3 + x^4 - 2x^5 - 3x^6 + 2x^7 + 2x^8 + x^9$$

has degree 9. And the information rate is :

$$\frac{k}{n} = \frac{162}{171} > {}^3/_4 .$$

Thus the negacyclic codes generated by these generator polynomials form a class which has rates

$$\frac{k}{n} \geq \frac{p-1}{p+1} = 3/4 .$$

2-3. NEGACYCLIC CODES with $n \neq \frac{p^r - 1}{2}$.

The negacyclic codes discussed previously have all lengths $\nu = \frac{p^r - 1}{2}$. Now we discuss the negacyclic codes with lengths $n \neq \frac{p^r - 1}{2}$.

To find $g(x)$ for such codes we proceed as follows :

For a given n and a given p, let c be the odd positive integer such that $nc = \frac{p^r - 1}{2}$. Then $g(x)$ can be found from the following

Theorem 2 : If the roots of $g(x)$ include $\alpha^c, \alpha^{3c}, \ldots, \alpha^{(2t-1)c}$, where $2t-1 < p$, then the negacyclic code of length n can correct any error pattern of Lee weight t or less and α is a primitive element of $GF(p^r)$.

This theorem follows directly from the theorem given previously for negacyclic codes with length $\nu = \frac{p^r - 1}{2}$. The restriction that c is odd is necessary since if c is not odd then $x^n + 1$ will not divide $x^\nu + 1$.

EXAMPLE 4 . If $p = 5$ and $r = 2$, we have $\nu = \frac{p^r - 1}{2} = 12$. If $n = 4$, then $4 \cdot 3 = 12$ so that $c = 3$. The polynomial $x^2 - 2$ has $\alpha^c = \alpha^3$ as a root . Therefore, if we make $g(x) = x^2 - 2$, then this $g(x)$ generates a $(4, 2)$ negacyclic code with $t = 1$.

We have included in Appendix B a list of generator polynomials for negacyclic codes of certain lengths .

2-4 . NEGACYCLIC CLASSES .

In the case of cyclic codes , a code word and all of its cyclic shifts are said to constitute a CYCLIC CLASS . The number N_i of distinct elements in any cyclic class S_i can be only n or a factor of n , where n is the length of the code . FOR EXAMPLE, if $n = 63$, then N_i can be only 1, 3, 7, 9, 21, or 63 .

Similarly, in the case of negacyclic codes we can define a code word and all its negacyclic shifts as constituting a NEGACYCLIC CLASS .

Suppose T_j is the operator indicating the negacyclic shift by j positions . Then, for any negacyclic code word $V(x)$, we have $T_n V(x) = -V(x)$ and $T_{2n} V(x) = T_n(-V(x)) = V(x)$.

In view of this we can say that the number of distinct elements in a negacyclic class can be only $2n$ or a factor of $2n$.

Totally there are $q^k - 1$ non-zero words. Barring the all-zero word which is a negacyclic class with one element, suppose every negacyclic class has $2n = p^r - 1$ distinct elements. Then $p^r - 1$ divides $q^k - 1$, implying that k is divisible by r. From this it also follows that if r does not divide k, then $p^r - 1$ does not divide $q^k - 1$, indicating thereby that not all negacyclic classes have $2n$ distinct elements.

EXAMPLE 5. We consider the $(4, 2, 1)$ negacyclic code generated by $g(x) = x^2 - 2$ over $GF(5)$, we get 3 negacyclic classes shown below.

$$\begin{matrix} -2 & 0 & 1 & 0 \\ 0 & -2 & 0 & 1 \\ -1 & 0 & -2 & 0 \\ 0 & -1 & 0 & -2 \\ 2 & 0 & -1 & 0 \\ 0 & 2 & 0 & -1 \\ 1 & 0 & 2 & 0 \\ 0 & 1 & 0 & 2 \end{matrix} \qquad (.1)$$

$$\begin{matrix} -2 & -2 & 1 & 1 \\ -1 & -2 & -2 & 1 \\ -1 & -1 & -2 & -2 \\ 2 & -1 & -1 & -2 \\ 2 & 2 & -1 & -1 \\ 1 & 2 & 2 & -1 \\ 1 & 1 & 2 & 2 \\ -2 & 1 & 1 & 2 \end{matrix} \qquad (2)$$

$$\begin{matrix} -1 & 0 & 2 & 0 \\ 0 & -1 & 0 & 2 \\ -2 & 0 & -1 & 0 \\ 0 & -2 & 0 & -1 \\ 1 & 0 & -2 & 0 \\ 0 & 1 & 0 & -2 \\ 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{matrix} \qquad (3)$$

2-5. DECODING OF NEGACYCLIC CODES

While the decoding of negacyclic codes can be done using methods parallel to those use in the case of BCH codes, there are some differences in detail. These differences arise because of the fact that, whereas in the case of BCH codes the

weight of the error in any position of the word is 0 or 1, the weight of the error in the case of negacyclic cedes can be $0, \pm 1, \pm 2, \ldots$ or $\pm t$. A consequence of this fact is that the error locator polynomial in the case of negacyclic codes can have repeated roots whereas in the case of BCH codes such a situation is not possible.

Next we give a few details about the decoding of negacyclic codes with $t = 1$, and $t = 2$, which are of practical importance.

2-5.1. Case of $t = 1$

If $t = 1$, then the error polynomial $E(x) = 0$ or ax^b, where $|a| \leq 1$ and $b \leq n-1$

Given $R(x) = V(x) + E(x)$,

where $V(x)$ belongs to V and $|E(x)| \leq 1$, we compute $R(\alpha)$ and express it in the form

$$R(\alpha) = a\alpha^b$$

The error $E(x)$ is formed using the facts that

$$\{R(\alpha) = 0\} \iff \{E(x) = 0\},$$

$$\{R(\alpha) = a\alpha^b\} \iff \{E(x) = ax^b\}.$$

The basis for these assertions is that since $\alpha^b \neq 0$,

$\{R(\alpha) = 0\} \iff \{a = 0\}$.

2-5.2. Case of $t = 2$

If $t = 2$, then

$$E(x) = a_i x^i + a_j x^j ,$$

where $|a_i| + | \leq 2$ and $i,j \leq n-1$

Given

$$R(x) = V(x) + E(x) ,$$

we compute $R(\alpha)$ and $R(\alpha^3)$.

To start the analysis we note that

$$R(\alpha) = a_i \alpha^i + a_j \alpha^j ,$$

$$R(\alpha^3) = a_i \alpha^{3i} + a_j \alpha^{3j} .$$

If $E(x) = 0$, then $a_i = -a_j$ and $i = j$. This means that $R(x) = 0$. On the other hand, if $R(\alpha) = 0$, then $a_i \alpha^i = -a_j \alpha^j = a_j \alpha^{n+j}$, implying that $a_i = a_j$ and $i = n+j$. But i can never exceed n-1. That is $a_i = a_j = 0$. Thus we have proved that

$$\{R(\alpha) = 0\} \Longleftrightarrow \{E(x) = 0\}$$

Now we consider the case of $|E(x)| = 1$, then $R^3(\alpha) = R(\alpha^3)$ since $a_i^3 = a_i$ and $a_j = 0$. On the other hand, suppose $R^3(\alpha) = R(\alpha^3)$. Then we have $(a_i \alpha^i + a_j \alpha^j)^3 = a_i \alpha^{3i} + a_j \alpha^{3j}$ or

$$a_i^3 \alpha^{3i} + 3a_i^2 \alpha^{2i} a_j \alpha^j + 3a_i \alpha^i a_j^2 \alpha^{2j} + a_j^3 \alpha^{3j}$$

$$= a_i \alpha^{3i} + a_j \alpha^{3j} ,$$

or

$$(a_i^3 - a_i)\alpha^{3i} + (a_j^3 - a_j)\alpha^{3j} + 3a_i a_j \alpha^{i+j} (a_i \alpha^i + a_j \alpha^j) = 0$$

Now if $a_j = 0$, then we have $a_i^3 - a_i = a_i(a_i^2 - 1) = 0$

or

$$a_i^2 = 1$$

or

$$a_i = \pm 1 .$$

On the other hand if $|a_i| = |a_j| = 1$, then we have

$$3\, a_i a_j\, \alpha^{i+j} (a_i \alpha^i + a_j \alpha^j) = 0$$

which means that

$$a_i \alpha^i + a_j \alpha^j = 0 .$$

or

$$R(\alpha) = 0$$

But this implies that $E(x) = 0$ which is against our supposition.

Thus we are left with the only possibility that $|a_j| = 1$ and $a_j = 0$.

In short we have proved that

$$\left.\begin{array}{l} R^3(\alpha) = R(\alpha^3) \\ R(\alpha) = \pm \alpha^i,\ i \le n-1 \end{array}\right\} \Longleftrightarrow \{E(x) = \pm x^i\}$$

Next we consider the case when $E(x) = \pm 2x^i$, where $i \le n-1$. If $E(x) = \pm 2x^i$, then $R^3(\alpha) = 4\, R(\alpha^3)$. On the other hand if $R^3(\alpha) = 4\, R(\alpha^3)$, then we have

$$(a_i^3 - 4a_i)\, \alpha^{3i} + (a_j^3 - 4a_j)\, \alpha^{3j} + 3a_i a_j\, \alpha^{i+j} (a_i \alpha^i + a_j \alpha^j) = 0$$

Now if $a_j = 0$, then we have $a_i(a_i^2 - 4) = 0$, or $a_i = \pm 2$. On the

other hand if $|a_i| = |a_j| = 1$, we have

$$-3a_i\alpha^{3i} - 3a_j\alpha^{3j} + 3a_ia_j\alpha^{i+j}(a_i\alpha^i + a_j\alpha^j) = 0$$

or

$$-R(\alpha^3) + a_ia_j\alpha^{i+j}R(\alpha) = 0$$

or

$$R(\alpha^3) + a_ia_j\alpha^{i+j}R(\alpha).$$

But $R^3(\alpha) = 4R(\alpha^3)$ by supposition. This means that $a_ia_j = 4$ and $\alpha^{i+j} = 1$ which are again against our supposition. Therefore we are left with the only possibility that $a_i = \pm 2$ and $a_j = 0$. In short we have proved that

$$\left.\begin{array}{l} R^3(\alpha) = 4R(\alpha^3), \\ R(2) = \pm 2\alpha^i,\ i \le n-1 \end{array}\right\} \Longleftrightarrow \{E(x) = \pm 2x^i\}$$

The final case to be considered is when $E(x) = a_ix^i + a_jx^j$, $|a_i| = |a_j| = 1$. In such a case we have

$$R(\alpha^3) = R(\alpha)[a_i^2\alpha^{2i} + a_j^2\alpha^{2j} - a_ia_j\alpha^{i+j}]$$

$$= R(\alpha)[(a_i\alpha^i + a_j\alpha^j)^2 - 3a_ia_j\alpha^{i+j}]$$

$$= R(\alpha)[R^2(\alpha) - 3a_ia_j\alpha^{i+j}]$$

or

$$3a_ia_j\alpha^{i+j} = \frac{R^3(\alpha) - R(\alpha^3)}{R(\alpha)}$$

Starting with

$$R(\alpha) = a_i \alpha^i + a_j \alpha^j ,$$

we have

$$3a_i \alpha^i R(\alpha) = 3a_i^2 \alpha^{2i} + 3a_i a_j \alpha^{i+j}$$

or

$$3a_i \alpha^i R(\alpha) = 3a_i^2 \alpha^{2i} + \frac{R^3(\alpha) - R(\alpha^3)}{R(\alpha)}$$

or

$$3\alpha^{2i} - 3a_i \alpha^i R(\alpha) + \frac{R^3(\alpha) - R(\alpha^3)}{R(\alpha)} = 0$$

where $a_i = \pm 1$. Taking any one of these two values of a_i, we get the roots of this quadratic. The roots give the error $E(x)$.

EXAMPLE 6. Suppose $g(x) = x^4 + x^3 - 2x + 1$ which generates an $(n = \frac{5^2 - 1}{2} = 12,\ k = 12 - 4 = 8)$ negacyclic code with $t = 2$. Let $E(x) = x^5 - x^8$. We use Table 2 below for computation.

Table 2. Non-zero elements of $GF(5^2)$, α is a root of $p(x) = x^2 + x + 2$.

α^0	$= 1$	α^{12}	$= -1$
α^1	$= \alpha$	α^{13}	$= -\alpha$
α^2	$= -2 - \alpha$	α^{14}	$= 2 + \alpha$
α^3	$= 2 - \alpha$	α^{15}	$= -2 + \alpha$

$$\alpha^4 = 2 - 2\alpha \qquad \alpha^{16} = -2 + 2\alpha$$

$$\alpha^5 = -1 - \alpha \qquad \alpha^{17} = 1 + \alpha$$

$$\alpha^6 = 2 \qquad \alpha^{18} = -2$$

$$\alpha^7 = 2\alpha \qquad \alpha^{19} = -2\alpha$$

$$\alpha^8 = 1 - 2\alpha \qquad \alpha^{20} = -1 + 2\alpha$$

$$\alpha^9 = -1 - 2\alpha \qquad \alpha^{21} = 1 + 2\alpha$$

$$\alpha^{10} = -1 + \alpha \qquad \alpha^{22} = 1 - \alpha$$

$$\alpha^{11} = -2 - 2\alpha \qquad \alpha^{23} = 2 + 2\alpha$$

Then,

$$E(\alpha) = \alpha^5 - \alpha^8 = (-1 - \alpha) - (1 - 2\alpha) = -2 + \alpha = \alpha^{15}$$

$$E(\alpha^3) = \alpha^{15} - \alpha^{24} = (-2 + \alpha) - 1 = 2 + \alpha = \alpha^{14}$$

Now, given $E(\alpha)$ and $E(\alpha^3)$, we proceed to get back $E(x)$. We note that since $R(\alpha) = E(\alpha)$ and $R(\alpha^3) = E(\alpha^3)$, for the purpose of example, there is no need to assume any $V(x)$.

Since $R(\alpha) \neq 0$, $E(\alpha) \neq 0$.

Next,

$$E(\alpha^3) = \alpha^{45} = \alpha^{21},$$

which is not equal to $E(\alpha^3)$. Therefore $|E(x)| > 1$.

Also, $4E(\alpha^3) = 4\alpha^{14} = -\alpha^{14} = \alpha^2$ which is not equal to $E^3(\alpha)$. Therefore $E(x) \neq \pm 2x^i$.

Thus $E(x) = a_i x^i + a_j x^j$, $|a_i| = 1$, $|a_j| = 1$.

2-5.3. Case of $t \geq 3$.

For $t \geq 3$, the type of arguments used for $t = 1$ and 2 can still be used, but the procedure becomes too involved. It would be much simpler to use the general decoding procedure of Berlekamp [5].

2-6. PERMUTATION DECODING [10].

Let V be an (n, k, t) negacycliccode over GF(p) with $g(x)$ as its generator polynomial with $|E(x)| \leq t$. Starting with

$$E(x) = g(x)\, A(x) + E_1(x),$$

where $E_1(x)$ is the remainder, we note that $E(x) - E_1(x)$ is a code word. This implies that $|E_1(x)| > t$ or $E(x) = E_1(x)$. In the latter case $E(x)$ has degree n-k-1 or less since $E_1(x)$ is the remainder. Thus we have proved the following known

Theorem 3 : $E(x)$ modulo $g(x)$ has weight t_0 or less if and only if $E(x)$ is confined to the first n-k positions.

On the basis of this theorem and the fact that a negacyclic shift of a polynomial does not alter the weight of the polynomial, we can say that if

$$\left| \left[T_j E_1^{p^q}(x) \right] \text{ modulo } g(x) \right| \leq t ,$$

where T_j is the operator indicating the j^{th} negacyclic shift to the right, and q, some integer,

$$E(x) = \left\{ (-T_j) \left\{ \left[T_j E_1^{p^q}(x) \right] \text{ modulo } g(x) \right\} \right\}^{p^{\frac{1}{q}}}$$

where $(-T_j)$ is the operator indicating the j^{th} negacyclic shift to the left.

If there are a j and a q such that

$$\left| T_j E_1^{p^q}(x) \text{ modulo } g(x) \right| \leq t$$

for every possible E(x) with $|E(x)| \leq t$, then V is said to be PERMUTATION DECODABLE. If the maximum value of q required is s-1, then V is said to be s-step permutation decodable.

The question that now arises naturally is under what condition V is permutation decodable. In this connection we note that 1-step permutation decodability depends on the spacing between adjacent terms in E(x) and not on the weights of the individual terms, a condition that is relevant to the permutation decodability of cyclic codes also. From this fact it follows that whatever results are valid for 1-step permutation decodability of cyclic codes are also valid for negacyclic codes.

In view of this , we give below the result which is carried over from cyclic codes .

Theorem 4 : If $\frac{k}{n} < \frac{1}{t}$, then V is one-step-permutation decodable .

EXAMPLE 7 . For $p = 5$, we have $n = 12$. The generator polynomial .

$$g(x) = x^8 + 2x^6 + 2x^2 - 1$$

generates a code with $t = 2$. The value of $k = 12 - 8 = 4$. Thus

$$\frac{k}{n} = \frac{4}{12} = \frac{1}{3} < \frac{1}{2} = \frac{1}{t} .$$

This code is , therefore , 1-step permutation decodable .

Let us take the code word as

$$V(x) = x^8 + 2x^6 + 2x^2 - 1 .$$

Suppose that the received word has two errors such as

$$R(x) = 2x^2 + 2x^6 + x^8 + x^9 .$$

Let

$$E_1(x) = R(x) \bmod g(x)$$

$$= 1 + x - 2x^3 - 2x^7 .$$

Now we perform successively the shifting $E_1(x)$ and taking

modulo g(x) after each shifting until

$$\left| [\, T_j \, E_1(x) \,] \bmod g(x) \right| \leq t = 2 .$$

Such as

$$\left| [\, T_1 \, E_1(x) \,] \bmod g(x) \right| = \left| -2 + x - 2x^4 - x^6 \right| > 2$$

$$\vdots$$

$$\left| [\, T_3 \, E_1(x) \,] \bmod g(x) \right| = \left| -1 + x^3 \right| = 2 .$$

Next we find E(x) by

$$E(x) = (-T_3)(-1 + x^3)$$

$$= x^{-3}(-1 + x^3) = -x^{-3} + 1$$

$$= x^9 + 1 ,$$

that is exactly what we expect to be .

2-7 . SYNCHRONIZATION [5] .

A code which can correct the simultaneous occurence of slip (synchronization error) and additive (channel) error is called a synchronizable error-correcting code . The problem of constructing and decoding of such codes has been extensively studied . The codes are basically cyclic codes which are modified suitably .

It is interesting to note that the techniques known in the case of cyclic codes can be used also for negacyclic codes with little or no modification . To illustrate this comment we next discuss the application of a technique , developed for cyclic codes , to negacyclic codes .

The synchronization problem is as follows :

Suppose we have three code words in succession as shown below

$$a_0 a_1 a_2 \cdots a_{n-1} b_0 b_1 \cdots b_{n-1} c_0 c_1 c_2 \cdots c_{n-2} c_{n-1} .$$

At the receiving end when we partition (frame) this sequence into blocks of n digits , we may make a mistake such as :

$$a_0 a_1 \{ a_2 \cdots [a_{n-1} b_0 b_1 \cdots b_{n-2}] b_{n-1} c_0 c_1 \} c_2 \cdots c_{n-1} .$$

This mistake is called a synchronization-error , slip or mis-framing . FOR EXAMPLE , with reference to the figure , $[a_{n-1} b_0 \cdots b_{n-2}]$ has a left slip by one position and $\{ a_2 \cdots c_1 \}$ has a right slip by two positions. It is to be assumed that the magnitude of the slip is less than or equal to, some preassigned value s .

Let V be an (n, k, t) negacyclic code generated by g(x) . Let V' be the (n, k') subcode generated by $g(x)g_1(x)$

where $g_1(x)$ is irreducible, $(g_1(x), g(x)) = 1$, $g_1(x)$ divides $x^{\varepsilon} + 1$ and not $x^{\varepsilon'} + 1$ for $\varepsilon' < \varepsilon$, and $x^{\varepsilon} + 1$ divides $x^n + 1$.

Let $W(x)$ be defined by

$$W(x) = V'(x) + g(x) .$$

Let W be the set of all possible code words $W(x)$. We note that W is (n, k').

Since $W(x) = g(x)g_1(x)\,C(x) + g(x)$

$$= g(x)[\, g_1(x)C(x) + 1 \,],$$

from which we see that $W(x)$ modulo $g(x)$ is zero and $W(x)$ modulo $g_1(x)$ is not zero, we have the result that

$$W \subset V - V' .$$

Suppose $A(x)$ corresponding to $a_0 a_1 a_2 \cdots a_{n-1}$ belongs to W. Suppose we prefix and suffix this in the way shown below

$$-a_{n-i}\,-a_{n-i+1} \cdots -a_{n-1}\; a_0 \cdots a_{n-1}\; -a_0\, -a_1 \cdots -a_{i-1} .$$

Suppose we transmit this block of $n+2i$ digits over a channel. We assume that at the receiving end we get a corrupted version of this.

If we now pick n consecutive digits, we see that this block B of n digits is a negacyclically shifted version of $a_0 a_1 a_2 \ldots\ldots\ldots a_{n-1}$ plus errors caused by the channel. Let us assume that this error pattern is of weight t or less. Under this condition the error can be corrected, since B belongs to V. After such correction what we have is

$$B(x) = x^j A(x) \text{ modulo } x^n + 1 .$$

Where we still have to determine j. Writing

$$x^j A(x) = (x^n + 1)D(x) + B(x) ,$$

we note that

$$\begin{aligned} B(x) \bmod g_1(x) &= x^j A(x) \bmod g_1(x) \\ &= x^j g(x) \bmod g_1(x) , \end{aligned}$$

since $x^j A(x)$ has the form

$$x^j A(x) = x^j g(x)[\, g_1(x)\, F(x) + 1\,].$$

Now let us see under what condition $x^j g(x) \bmod g_1(x)$ is distinct for each j. To do this, let us consider

$$x^{j_1} g(x) = g_1(x) L_1(x) + M(x) ,$$

$$x^{j_2} g(x) = g_1(x) L_2(x) + M(x) ,$$

from which we get

$$g(x)\, x^{j_1} (1 - x^{j_2 - j_1}) = g_1(x) [L_1(x) - L_2(x)],$$

where we assume $j_2 > j_1$. This means that $g_1(x)$ divides $1 - x^{j_2 - j_1}$. Since $g_1(x)$ divides $1 + x^{\varepsilon}$ and not $1 + x^{\varepsilon'}$ for any $\varepsilon' < \varepsilon$, we conclude that $g_1(x)$ has exponent 2ε. Therefore, if $j_2 - j_1 < 2\varepsilon$, then $g_1(x)$ can not divide $1 - x^{j_2 - j_1}$. To differentiate between left slip and right slip, if we make $2(\text{slip}) < \varepsilon$, then

$x^j g(x) \bmod g_1(x)$ is distinct for each j.

To summarize the discussion, if we store

$$x^j g(x) \bmod g_1(x) \quad \text{for } j = 0, 1, 2, \ldots, \varepsilon - 1,$$

then by computing $x^s B(x) \bmod g(x)$ and comparing it with the stored quantities, we can find the magnitude and direction of the slip.

2-8. MAJORITY-LOGIC-DECODING [12].

As is well-known majority-logic-decoding is one of the simplest decoding techniques known. In regard to

negacyclic codes one of the open problems is to find majority-logic-decodable codes which are negacyclic or derived from negacyclic codes. While no general results seem to be available in this direction, the following code of GF(5) is of interest :

EXAMPLE 8. Let us start with the negacyclic code which has $p = 5$ and $r = 2$ so that $n = \frac{p^r - 1}{2} = 12$ and $t = \frac{p - 1}{2} = 2$. The generator polynomial of this code may be

$$g_1(x) = (x^2 - 2x + 3)(x^2 + 2) = x^4 - 2x^3 + x + 1 .$$

Let V be the (11, 4) shortened subset generated by

$$g(x) = g_1(x)(1 - x + 2x^3)$$
$$= 1 - x^2 - x^5 + x^6 + 2x^7 .$$

Every word V(x) of V can be expressed in the form

$$V(x) = g(x)\, C(x)$$
$$= (1 - x^2 - x^5 + x^6 + 2x^7)(c_0 + c_1x + c_2x^2 + c_3x^3)$$
$$= c_0 + c_1x + (c_2 - c_0)x^2 + (c_3 - c_1)x^3 - c_2x^4$$
$$- (c_0 + c_3)x^5 + (c_0 - c_1)x^6 + (2c_0 + c_1 - c_2)x^7$$
$$+ (2c_1 + c_2 - c_3)x^8 + (2c_2 + c_3)x^9 + 2c_3x^{10} .$$

A received word is:

$$R(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{10} x^{10}$$

To decode R(x), we equate the corresponding coefficients of V(x) and R(x) such as:

$$\begin{aligned}
r_0 &= c_0 \\
r_1 &= c_1 \\
r_2 &= -c_0 + c_2 \\
r_3 &= -c_1 + c_3 \\
r_4 &= -c_2 \\
r_5 &= -c_0 - c_3 \qquad \text{(Ia)} \\
r_6 &= c_0 - c_1 \\
r_7 &= 2c_0 + c_1 - c_2 \\
r_8 &= 2c_1 + c_2 - c_3 \\
r_9 &= 2c_2 + c_3 \\
r_{10} &= 2c_3
\end{aligned}$$

Combining these equations we get

$$\begin{aligned}
2c_0 &= 2r_0 \\
2c_0 &= -2r_2 - 2r_4 \\
2c_0 &= 2r_1 + 2r_6 \qquad \text{(Ib)} \\
2c_0 &= -2r_5 - r_{10} \\
2c_0 &= r_7 + 2r_8 + 2r_9
\end{aligned}$$

We estimate c_0 by taking a majority vote , that is we consider c_0 is correct if it agrees with at least 3 out of 5 equations above .

After getting c_0 , we subtract $c_0 g(x)$ from the received polynomial and shift the sum to the left by one position to get $r'_0 + r'_1 x + r'_2 x^2 + \ldots + r'_{n-2} x^{n-2}$. Then we refer back to set (Ib) to estimate c_1 instead of c_0 by using r'_j instead of r_j .

Clearly the process can be repeated to get all of the c_i's .

EXAMPLE 9 . Here we repeat the example 8 with details . We suppose that the information polynomial C(x) is :

$$C(x) : 1 + 2x - x^2 + x^3 .$$

Then the corresponding code word is :

$$V(x) = C(x)g(x)$$

$$= 1 + 2x - 2x^2 - x^3 + x^4 - 2x^5 - x^6 + 2x^8 - x^9 + 2x^{10} .$$

And we assume there are two errors at positions 3 and 8 (increasing positions from left to right), that is the received word having form :

$$R(x) = 1 + 2x - x^2 - x^3 + x^4 - 2x^5 - x^6 + x^7 + 2x^8 - x^9 + 2x^{10}$$

which gives the set of r_j's values :

$r_0 = 1$ $\quad$ $r_6 = -1$

$r_1 = 2$ $\quad$ $r_7 = 1$

$r_2 = -1$ $\quad$ $r_8 = 2$

$r_3 = -1$ $\quad$ $r_9 = -1$

$r_4 = 1$ $\quad$ $r_{10} = 2$

$r_5 = -2$

Combining these r_j's with set (Ib) to estimate c_0 :

$2c_0 = 2r_0 = 2 \longrightarrow c_0 = 1$

$2c_0 = -2r_2 - 2r_4 = 0 \longrightarrow c_0 = 0$

$2c_0 = -2r_5 - r_{10} = 2 \longrightarrow c_0 = 1$

$2c_0 = 2r_1 + 2r_6 = 2 \longrightarrow c_0 = 1$

$2c_0 = r_7 + 2r_8 + 2r_9 = -2 \longrightarrow c_0 = -1$

We see that $c_0 = 1$ is agreeable to majority (3 out of 5), thus we take $c_0 = 1$.

Next we subtract $c_0 g(x) = g(x)$ from $R(x)$ we get :

$$R_1(x) = R(x) - g(x)$$

$$= 2x - x^3 + x^4 - x^5 - 2x^6 - x^7 + 2x^8 - x^9 + 2x^{10}$$

Then we shift $R_1(x)$ to the left one position

$$R'(x) = x^{-1} R_1(x) = 2 - x^2 + x^3 - x^4 - 2x^5 - x^6 + 2x^7 - x^8 + 2x^9$$

Now we use the set (Ib) to estimate c_1 by replacing c_0 by c_1 and r_j by r'_j. We obtain

$$2c_1 = 2r'_0 = 4$$

$$2c_1 = -2r'_2 - 2r'_4 = 4$$

$$2c_1 = -2r'_5 - r'_{10} = 4$$

$$2c_1 = 2r'_1 + 2r'_6 = -2$$

$$2c_1 = r'_7 + 2r'_8 + 2r'_9 = 4$$

thus $c_1 = 2$.

Similarly,

$$R''(x) = (-T_1)[R'(x) - c_1 g(x)]$$

$$= 0 + x + x^2 - x^3 + 0 + 2x^5 - 2x^6 - x^7 + 2x^8,$$

which gives $c_2 = -1$.

And

$$R'''(x) = (-T_1)[R''(x) - c_2 g(x)]$$

$$= 1 + 0 - x^2 + 0 + x^4 - x^5 + x^6 + 2x^7,$$

which gives $c_3 \cong 1$.

The values of estimated c_i's are now used to recompute r_j's in set (Ia), then the corrected $R^*(x)$ is indeed $V(x)$.

CONCLUDING REMARKS

In this thesis we have discussed negacyclic codes.

From the discussion in Chapter 2 it is clear that negacyclic codes are very much similar to cyclic codes and that, in fact, techniques developed for cyclic codes can easily be adapted to negacyclic codes.

Regarding implementation, negacyclic codes are somewhat less simple in the sense that the signs of the digits shifted beyond the last position have to be changed. This is not necessary in the case of cyclic codes.

It may be worthwhile to investigate further the problem of majority-logic-decodable negacyclic codes.

APPENDIX A

--------oOo --------

SOME RESULTS ABOUT GENERATOR POLYNOMIALS FOR NEGACYCLIC CODES

A negacyclic code can be constructed from a generator polynomial.

In obtaining a generator polynomial, there are several steps to follow :

1. For a given prime p and a given r, the maximum error-correcting capability t and the block length n are given by:

$$t = \frac{p - 1}{2} ,$$

$$n = \frac{p^r - 1}{2} .$$

2. Decompose $x^n + 1$ into

$$x^n + 1 = Q(x) . Re(x)$$

where

$$Q(x) = I_1(x) . I_2(x) . \ldots . I_m(x) ,$$

the degree of $I_i(x)$ is r.

$Re(x)$ is the remainder polynomial whose degree is less than r.

3. Identify primitive polynomials by calculating the order of roots of polynomials which are factors of $Q(x)$. If a polynomial whose root has order $2n = p^r - 1$ then it is a primitive polynomial.

4. Construct a table listing all non-zero elements in $GF(p^r)$ for each primitive polynomial chosen.

5. Compute the generator polynomial

$$g(x) = \mathrm{LCM}\{ \prod_{j=0}^{r-1} (\prod_{i=1,3,..}^{p-2} (x - \alpha^{i \cdot p^j})) \}$$

by referring to table in part (4).

Note:

i. One generator polynomial can be obtained from each primitive polynomial. For each pair of p and r, there are more than one primitive polynomial and therefore more than one generator polynomial.

ii. Where there is a vector of form $(v_0, v_1, \ldots, v_r)$ we understand that it is a polynomial of increasing power whose elements associate with coefficients of the polynomial. FOR EXAMPLE, a vector (-3, 2, 0, 1)is interpreted as a

polynomial $-3 + 2x + 0x^2 + x^3$.

iii. Where there is an expression $a^i = a_0 a_1 \ldots a_{r-1}$ we understand that a^i is a function of $a^0, a^1, a^2, \ldots, a^{r-1}$ with elements a_j's. FOR EXAMPLE, $a^8 = 1\ -2\ 0$ is interpreted as

$$a^8 = 1 - 2a + 0a^2 .$$

Followings are the results obtained for :

$p = 5$, $r = 2$

$p = 5$, $r = 3$

$p = 7$, $r = 2$

$p = 7$, $r = 3$

$p = 11$, $r = 2$

$p = 13$, $r = 2$

A=1.

For $p = 5$, $r = 2$ then $t = 2$ and $n = 12$.

Irreducible polynomials	Root order
$1 + x^{12} = (2 + 0x + x^2)$	8
$(-2, 0, 1)$	8
$(-2, 2, 1)$	24*
$(-2, -2, 1)$	24*
$(2, 1, 1)$	24*
$(2, -1, 1)$	24*

* indicates the corresponding polynomial is primitive

GF(5^2) in terms of α, a root of $-2-2x+x^2$.

$\alpha = 1\ 0$	$\alpha^{12} = -1\ 0$
$\alpha^1 = 0\ 1$	$\alpha^{13} = 0\ -1$
$\alpha^2 = 2\ 2$	$\alpha^{14} = -2\ -2$
$\alpha^3 = -1\ 1$	$\alpha^{15} = 1\ -1$
$\alpha^4 = 2\ -1$	$\alpha^{16} = -2\ -1$
$\alpha^5 = 2\ -1$	$\alpha^{17} = -2\ 1$
$\alpha^6 = -2\ 0$	$\alpha^{18} = 2\ 0$
$\alpha^7 = 0\ -2$	$\alpha^{19} = 0\ -2$
$\alpha^8 = 1\ 1$	$\alpha^{20} = -1\ -1$

$\alpha^9 = 2\ -2$	$\alpha^{21} = -2\ \ 2$
$\alpha^{10} = 1\ -2$	$\alpha^{22} = -1\ \ 2$
$\alpha^{11} = 1\ \ 2$	$\alpha^{23} = -1\ -2$

The corresponding generator polynomial is:

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

A-2.

For p=5 , r = 3 then t= 2 and n = 62 .

$1 + x^{62}$	Irreducible polynomials	Root order
$\doteq$	$(-2 \ -x \ -2x^2 \ +x^3)$	124^*
	(-2, 2, -2, 1)	124^*
	(-2, 0, -1, 1)	124^*
	(-2, -2, 0, 1)	124^*
	(-2, -1, 0, 1)	124^*
	(-2, -1, 1, 1)	124^*
	(-2, 1, 1, 1)	124^*
	(-2, 0, 2, 1)	124^*
	(-2, 1, 2, 1)	124^*
	(-2, 2, 2, 1)	124^*
	(2, 0, -2, 1)	124^*
	(2, 1, -2, 1)	124^*
	(2, 2, -2, 1)	124^*
	(2, -1, -1, 1)	124^*
	(2, 1, -1, 1)	124^*
	(2, -2, 0, 1)	124^*
	(2, -1, 0, 1)	124^*
	(2, 0, 1, 1)	124^*
	(2, -1, 2, 1)	124^*

(2, 2, 2, 1)	124*
(1, 0, 1, 0)	Re(x)

* indicates the corresponding polynomial is primitive .

GF(5^3) in terms of α , a root of $-2 - x^2 + x^3$.

$\alpha^0 = 1$	$\alpha^{42} = -2\ \ 2\ \ 1$	$\alpha^{84} = -1\ \ -1\ \ 0$
$\alpha^1 = 0\ \ 1$	$\alpha^{43} = 2\ \ -2\ \ -2$	$\alpha^{85} = 0\ \ -1\ \ -1$
$\alpha^2 = 0\ \ 0\ \ 1$	$\alpha^{44} = 1\ \ 2\ \ 1$	$\alpha^{86} = -2\ \ 0\ \ -2$
$\alpha^3 = 2\ \ 0\ \ 1$	$\alpha^{45} = 2\ \ 1\ \ -2$	$\alpha^{87} = 1\ \ -2\ \ -2$
$\alpha^4 = 2\ \ 2\ \ 1$	$\alpha^{46} = 1\ \ 2\ \ -1$	$\alpha^{88} = 1\ \ 1\ \ 1$
$\alpha^5 = 2\ \ 2\ \ -2$	$\alpha^{47} = -2\ \ 1\ \ 1$	$\alpha^{89} = 2\ \ 1\ \ 2$
$\alpha^6 = 1\ \ 2\ \ 0$	$\alpha^{48} = 2\ \ -2\ \ 2$	$\alpha^{90} = -1\ \ 2\ \ -2$
$\alpha^7 = 0\ \ 1\ \ 2$	$\alpha^{49} = -1\ \ 2\ \ 0$	$\alpha^{91} = 1\ \ -1\ \ 0$
$\alpha^8 = -1\ \ 0\ \ -2$	$\alpha^{50} = 0\ \ -1\ \ 2$	$\alpha^{92} = 0\ \ 1\ \ -1$
$\alpha^9 = 1\ \ -1\ \ -2$	$\alpha^{51} = -1\ \ 0\ \ 1$	$\alpha^{93} = -2\ \ 0\ \ 0$
$\alpha^{10} = 1\ \ 1\ \ 2$	$\alpha^{52} = 2\ \ -1\ \ 1$	$\alpha^{94} = 0\ \ -2\ \ 0$
$\alpha^{11} = -1\ \ 1\ \ -2$	$\alpha^{53} = 2\ \ 2\ \ 0$	$\alpha^{95} = 0\ \ 0\ \ -2$
$\alpha^{12} = 1\ \ -1\ \ -1$	$\alpha^{54} = 0\ \ 2\ \ 2$	$\alpha^{96} = 1\ \ 0\ \ -2$
$\alpha^{13} = -2\ \ 1\ \ -2$	$\alpha^{55} = -1\ \ 0\ \ -1$	$\alpha^{97} = 1\ \ 1\ \ -2$
$\alpha^{14} = 1\ \ -2\ \ -1$	$\alpha^{56} = -2\ \ -1\ \ -1$	$\alpha^{98} = 1\ \ 1\ \ -1$

$a^{15} = -2\ \ 1\ -2$

$a^{16} = -1\ -2\ -2$

$a^{17} = 1\ -1\ \ 1$

$a^{18} = 2\ \ 1\ \ 0$

$a^{19} = 0\ \ 2\ \ 1$

$a^{20} = 2\ \ 0\ -2$

$a^{21} = 1\ \ 2\ -2$

$a^{22} = 1\ \ 1\ \ 0$

$a^{23} = 0\ \ 1\ \ 1$

$a^{24} = 2\ \ 0\ \ 2$

$a^{25} = -1\ \ 2\ \ 2$

$a^{26} = -1\ -1\ -1$

$a^{27} = -2\ -1\ -2$

$a^{28} = 1\ -2\ \ 2$

$a^{29} = -1\ \ 1\ \ 0$

$a^{30} = 0\ -1\ \ 1$

$a^{31} = 2\ \ 0\ \ 0$

$a^{32} = 0\ \ 2\ \ 0$

$a^{33} = 0\ \ 0\ \ 2$

$a^{34} = -1\ \ 0\ \ 2$

$a^{35} = -1\ -1\ \ 2$

$a^{36} = -1\ -1\ \ 1$

$a^{57} = -2\ -2\ -2$

$a^{58} = 1\ -2\ \ 1$

$a^{59} = 2\ \ 1\ -1$

$a^{60} = -2\ \ 2\ \ 0$

$a^{61} = 0\ -2\ \ 2$

$a^{62} = -1\ \ 0\ \ 0$

$a^{63} = 0\ -1\ \ 0$

$a^{64} = 0\ \ 0\ -1$

$a^{65} = -2\ \ 0\ -1$

$a^{66} = -2\ -2\ -1$

$a^{67} = -2\ -2\ \ 2$

$a^{68} = -1\ -2\ \ 0$

$a^{69} = 0\ -1\ -2$

$a^{70} = 1\ \ 0\ \ 2$

$a^{71} = -1\ \ 1\ \ 2$

$a^{72} = -1\ -1\ -2$

$a^{73} = 1\ -1\ \ 2$

$a^{74} = -1\ \ 1\ \ 1$

$a^{75} = 2\ -1\ \ 2$

$a^{76} = -1\ \ 2\ \ 1$

$a^{77} = 2\ -1\ -2$

$a^{78} = 1\ \ 2\ \ 2$

$a^{99} = -2\ \ 1\ \ 0$

$a^{100} = 0\ -2\ \ 1$

$a^{101} = 2\ \ 0\ -1$

$a^{102} = -2\ \ 2\ -1$

$a^{103} = -2\ -2\ \ 1$

$a^{104} = 2\ -2\ -1$

$a^{105} = -2\ \ 2\ \ 2$

$a^{106} = -1\ -2\ -1$

$a^{107} = -2\ -1\ \ 2$

$a^{108} = -1\ -2\ \ 1$

$a^{109} = 2\ -1\ -1$

$a^{110} = -2\ \ 2\ -2$

$a^{111} = 1\ -2\ \ 0$

$a^{112} = 0\ \ 1\ -2$

$a^{113} = 1\ \ 0\ -1$

$a^{114} = -2\ \ 1\ -1$

$a^{115} = -2\ -2\ \ 0$

$a^{116} = 0\ -2\ -2$

$a^{117} = 1\ \ 0\ \ 1$

$a^{118} = 2\ \ 1\ \ 1$

$a^{119} = 2\ \ 2\ \ 2$

$a^{120} = -1\ \ 2\ -1$

$\alpha^{37} = 2\ -1\ 0$	$\alpha^{79} = -1\ 1\ -1$	$\alpha^{121} = -2\ -1\ 1$
$\alpha^{38} = 0\ 2\ -1$	$\alpha^{80} = -2\ -1\ 0$	$\alpha^{122} = 2\ -2\ 0$
$\alpha^{39} =$ -	$\alpha^{81} = 0\ -2\ -1$	$\alpha^{123} = 0\ 2\ -2$
$\alpha^{40} = 2\ -2\ 1$	$\alpha^{82} = -2\ 0\ 2$	$\alpha^{124} = 1$
$\alpha^{41} = 2\ 2\ -1$	$\alpha^{83} = -1\ -2\ 2$	

The corresponding generator polynomial is :

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

A-3 .

For $p = 7$, $r = 2$ then $t = 3$ and $n = 24$.

	Irreducible polynomials	Root order
$1 + x^{24} =$	$(-2 - 3x + x^2)$	48*
$-$	(-2 , -2 , 1)	48*
	(-2 , 2 , 1)	48*
	(-2 , 3 , 1)	48*
	(-1 , -3 , 1)	16
	(-1 , -1 , 1)	16
	(-1 , 1 , 1)	16
	(-1 , 3 , 1)	16
	(3 , -2 , 1)	48*
	(3 , -1 , 1)	48*
	(3 , 1 , 1)	48*
	(3 , 2 , 1)	48*

* indicates the corresponding polynomial is primitive .

GF (7^2) in terms of α, a root of $3 + x + x^2$.

$\alpha^0 = 1$	$\alpha^{16} = 2 \quad 0$	$\alpha^{32} = -3 \quad 0$
$\alpha^1 = 0 \quad 1$	$\alpha^{17} = 0 \quad 2$	$\alpha^{33} = 0 \quad -3$
$\alpha^2 = -3 \quad 1$	$\alpha^{18} = 1 \quad 2$	$\alpha^{34} = 2 \quad -3$
$\alpha^3 = -3 \quad -2$	$\alpha^{19} = 1 \quad 3$	$\alpha^{35} = 2 \quad -1$
$\alpha^4 = -1 \quad 2$	$\alpha^{20} = -2 \quad -3$	$\alpha^{36} = 3 \quad 1$
$\alpha^5 = 1 \quad 1$	$\alpha^{21} = 2 \quad 2$	$\alpha^{37} = -3 \quad -3$
$\alpha^6 = -3 \quad 2$	$\alpha^{22} = 1 \quad -3$	$\alpha^{38} = 2 \quad 1$
$\alpha^7 = 1 \quad -1$	$\alpha^{23} = 2 \quad -2$	$\alpha^{39} = -3 \quad -3$
$\alpha^8 = 3 \quad 0$	$\alpha^{24} = -1 \quad 0$	$\alpha^{40} = -2 \quad 0$
$\alpha^9 = 0 \quad 3$	$\alpha^{25} = 0 \quad -1$	$\alpha^{41} = 0 \quad -2$
$\alpha^{10} = -2 \quad 3$	$\alpha^{26} = 3 \quad -1$	$\alpha^{42} = -1 \quad -2$
$\alpha^{11} = -2 \quad 1$	$\alpha^{27} = 3 \quad 2$	$\alpha^{43} = -1 \quad -3$
$\alpha^{12} = -3 \quad -1$	$\alpha^{28} = 1 \quad -2$	$\alpha^{44} = 2 \quad 3$
$\alpha^{13} = 3 \quad 3$	$\alpha^{29} = -1 \quad -1$	$\alpha^{45} = 2 \quad -2$
$\alpha^{14} = -2 \quad -1$	$\alpha^{30} = 3 \quad -2$	$\alpha^{46} = -1 \quad 3$
$\alpha^{15} = 3 \quad -3$	$\alpha^{31} = -1 \quad 1$	$\alpha^{47} = -2 \quad 2$

The corresponding generator polynomial is :

$$g(x) = -1 + x - 3x^2 + x^3 - x^4 - 3x^5 + x^6 .$$

A-4.

For $p = 7$, $r = 3$ then $t = 3$ and $n = 171$.

$1 + x^{171} =$ Irreducible polynomials	Root order
$(-3 \ -3x \ -3x^2 \ +x^3)$	342*
(-3, 3, -3, 1)	342*
(-3, -1, -2, 1)	342*
(-3, 0, -2, 1)	342*
(-3, 2, -2, 1)	342*
(-3, 3, -2, 1)	342*
(-3, -3, -1, 1)	342*
(-3, -2, -1, 1)	342*
(-3, -1, -1, 1)	342*
(-3, 0, -1, 1)	342*
(-3, 0, 0, 1)	18
(-3, -2, 1, 1)	342*
(-3, 2, 1, 1)	342*
(-3, -1, 2, 1)	342*
(-3, 1, 2, 1)	342*
(-3, -2, 3, 1)	342*
(-3, 0, 3, 1)	342*
(-3, 1, 3, 1)	342*

(-3, 3, 3, 1)	342*
(1, -1, -3, 1)	114
(1, 0, -3, 1)	114
(1, 3, -3, 1)	38
(1, 1, -2, 1)	114
(1, 2, -2, 1)	114
(1, -3, -1, 1)	114
(1, 2, -1, 1)	114
(1, -3, 0, 1)	114
(1, 1, 0, 1)	114
(1, 2, 0, 1)	38
(1, -2, 1, 1)	114
(1, -1, 2, 1)	114
(1, 0, 2, 1)	38
(1, -3, 3, 1)	38
(1, 1, 3, 1)	38
(2, 2, -3, 1)	342*
(2, 3, -3, 1)	342*
(2, -3, -2, 1)	342*
(2, -2, -2, 1)	342*
(2, 3, -2, 1)	342*
(2, -1, -1, 1)	342*

(1, 0, 1, 1)	114
(1, 3, 1, 1)	38
(1, -2, 2, 1)	114
(2, 1, -1, 1)	342*
(2, 3, -1, 1)	342*
(2, -2, 0, 1)	342*
(2, -1, 0, 1)	342*
(2, 0, 0, 1)	18
(2, 3, 0, 1)	342*
(2, -2 1, 1)	342*
(2, 1, 1, 1)	342*
(2, -3, 2, 1)	342*
(2, -1, 2, 1)	342*
(2, -2, 3, 1)	342*
(2, -1, 3, 1)	342*
(2, 2, 3, 1)	342*
(1, 0, 0, 1)	6

*indicates the corresponding polynomial is primitive .

GF(7^3) interns of α, a root of $2 + 2x + 3x^2 + x^3$

$\alpha^0 = 1$	$\alpha^{114} = -3\ 0\ 0$	$\alpha^{228} = 2\ 0\ 0$
$\alpha^1 = 1$	$\alpha^{115} = 0\ -3\ 0$	$\alpha^{229} = 0\ 2\ 0$
$\alpha^2 = 1$	$\alpha^{116} = 0\ 0\ -3$	$\alpha^{230} = 0\ 0\ 2$
$\alpha^3 = -2\ -2\ -3$	$\alpha^{117} = -1\ -1\ 2$	$\alpha^{231} = 3\ 3\ 1$
$\alpha^4 = -1\ -3\ 0$	$\alpha^{118} = 3\ 2\ 0$	$\alpha^{232} = -2\ 1\ 0$
$\alpha^5 = 0\ -1\ -3$	$\alpha^{119} = 0\ 3\ 2$	$\alpha^{233} = 0\ -2\ 1$
$\alpha^6 = -1\ -1\ 1$	$\alpha^{120} = 3\ 3\ -3$	$\alpha^{234} = -2\ -2\ 2$
$\alpha^7 = -2\ -3\ 3$	$\alpha^{121} = -1\ 2\ -2$	$\alpha^{235} = 3\ 1\ -1$
$\alpha^8 = 1\ -1\ 2$	$\alpha^{122} = -3\ 3\ 1$	$\alpha^{236} = 2\ -2\ -3$
$\alpha^9 = 3\ -3\ 0$	$\alpha^{123} = -2\ 2\ 0$	$\alpha^{237} = -1\ 1\ 0$
$\alpha^{10} = 0\ 3\ -3$	$\alpha^{124} = 0\ -2\ 2$	$\alpha^{238} = 0\ -1\ 1$
$\alpha^{11} = -1\ -1\ -2$	$\alpha^{125} = 3\ 3\ -1$	$\alpha^{239} = -2\ -2\ 3$
$\alpha^{12} = -3\ 3\ -2$	$\alpha^{126} = 2\ -2\ -1$	$\alpha^{240} = 1\ -1\ 3$
$\alpha^{13} = -3\ 1\ 2$	$\alpha^{127} = 2\ -3\ 1$	$\alpha^{241} = 1\ 2\ -3$
$\alpha^{14} = 3\ 0\ 2$	$\alpha^{128} = -2\ 0\ 1$	$\alpha^{242} = -1\ 0\ -3$
$\alpha^{15} = 3\ -1\ 1$	$\alpha^{129} = -2\ 3\ -3$	$\alpha^{243} = -1\ -2\ 2$
$\alpha^{16} = -2\ 1\ 3$	$\alpha^{130} = -1\ -3\ -2$	$\alpha^{244} = 3\ 2\ -1$
$\alpha^{17} = 1\ -1\ -1$	$\alpha^{131} = -3\ 3\ 3$	$\alpha^{245} = 2\ -2\ -2$
$\alpha^{18} = 2\ 3\ 2$	$\alpha^{132} = 1\ -2\ 1$	$\alpha^{246} = -3\ -1\ -3$
$\alpha^{19} = 3\ -2\ -3$	$\alpha^{133} = -2\ -1\ 2$	$\alpha^{247} = -1\ 3\ 1$
$\alpha^{20} = -1\ 2\ 0$	$\alpha^{134} = 3\ 1\ 0$	$\alpha^{248} = -2\ -3\ 0$

$a^{21} = 0\ -1\ -2$

$a^{22} = 3\ \ 3\ \ 0$

$a^{23} = 0\ \ 3\ \ 3$

$a^{24} = 1\ \ 1\ \ 1$

$a^{25} = -2\ -1\ -2$

$a^{26} = -3\ \ 2\ -2$

$a^{27} = -3\ \ 1\ \ 1$

$a^{28} = -2\ \ 2\ -2$

$a^{29} = -3\ \ 2\ \ 1$

$a^{30} = -2\ \ 2\ -1$

$a^{31} = 2\ \ 0\ -2$

$a^{32} = -3\ -1\ -1$

$a^{33} = 2\ -1\ \ 2$

$a^{34} = 3\ -2\ \ 0$

$a^{35} = 0\ \ 3\ -2$

$a^{36} = -3\ -3\ \ 2$

$a^{37} = 3\ \ 0\ -2$

$a^{38} = -3\ \ 0\ -1$

$a^{39} = 2\ -1\ \ 3$

$a^{40} = 1\ \ 3\ -3$

$a^{41} = -1\ \ 0\ -2$

$a^{135} = 0\ \ 3\ \ 1$

$a^{136} = -2\ -2\ \ 0$

$a^{137} = 0\ -2\ -2$

$a^{138} = -3\ -3\ -3$

$a^{139} = -1\ \ 3\ -1$

$a^{140} = 2\ \ 1\ -1$

$a^{141} = 2\ -3\ -3$

$a^{142} = -1\ \ 1\ -1$

$a^{143} = 2\ \ 1\ -3$

$a^{144} = -1\ \ 1\ \ 3$

$a^{145} = 1\ \ 0\ -1$

$a^{146} = 2\ \ 3\ \ 3$

$a^{147} = 1\ \ 3\ \ 1$

$a^{148} = -2\ -1\ \ 0$

$a^{149} = 0\ -2\ -1$

$a^{150} = 2\ \ 2\ \ 1$

$a^{151} = -2\ \ 0\ -1$

$a^{152} = 2\ \ 0\ \ 3$

$a^{153} = 1\ \ 3\ -2$

$a^{154} = -3\ -2\ \ 2$

$a^{155} = 3\ \ 0\ -1$

$a^{249} = 0\ -2\ -3$

$a^{250} = -1\ -1\ \ 0$

$a^{251} = 0\ -1\ -1$

$a^{252} = 2\ \ 2\ \ 2$

$a^{253} = 3\ -2\ \ 3$

$a^{254} = 1\ -3\ \ 3$

$a^{255} = 1\ \ 2\ \ 2$

$a^{256} = 3\ -3\ \ 3$

$a^{257} = 1\ -3\ \ 2$

$a^{258} = 3\ -3\ -2$

$a^{259} = -3\ \ 0\ \ 3$

$a^{260} = 1\ -2\ -2$

$a^{261} = -3\ -2\ -3$

$a^{262} = -1\ \ 3\ \ 0$

$a^{263} = 0\ -1\ \ 3$

$a^{264} = 1\ \ 1\ -3$

$a^{265} = -1\ \ 0\ \ 3$

$a^{266} = 1\ \ 0\ -2$

$a^{267} = -3\ -2\ -1$

$a^{268} = 2\ -1\ \ 1$

$a^{269} = -2\ \ 0\ \ 3$

$a^{42} = -3\ \ 3\ -1$

$a^{43} = 2\ -1\ -1$

$a^{44} = 2\ -3\ \ 2$

$a^{45} = 3\ -2\ -2$

$a^{46} = -3\ \ 0\ -3$

$a^{47} = -1\ \ 3\ \ 2$

$a^{48} = 3\ \ 2\ -3$

$a^{49} = -1\ \ 2\ -3$

$a^{50} = -1\ -2\ -3$

$a^{51} = -2\ \ 0$

$a^{52} = 0\ \ 1\ -2$

$a^{53} = -3\ -3\ -2$

$a^{54} = -3\ \ 1\ \ 3$

$a^{55} = 1\ -2\ -1$

$a^{56} = 2\ \ 3\ \ 1$

$a^{57} = -2\ \ 0\ \ 0$

$a^{58} = 0\ -2\ \ 0$

$a^{59} = 0\ \ 0\ -2$

$a^{60} = -3\ -3\ -1$

$a^{61} = 2\ -1\ \ 0$

$a^{62} = 0\ \ 2\ -1$

$a^{156} = 2\ -2\ \ 3$

$a^{157} = 1\ \ 3\ \ 3$

$a^{158} = 1\ \ 2\ \ 1$

$a^{159} = -2\ -1\ -1$

$a^{160} = 2\ \ 0\ \ 2$

$a^{161} = 3\ -2\ \ 1$

$a^{162} = -2\ \ 1\ \ 2$

$a^{163} = 3\ \ 1\ \ 2$

$a^{164} = 3\ -1\ \ 2$

$a^{165} = 3\ -1\ \ 0$

$a^{166} = 0\ \ 3\ -1$

$a^{167} = 2\ \ 2\ -1$

$a^{168} = 2\ -3\ -2$

$a^{169} = -3\ -1\ \ 3$

$a^{170} = -3\ -2\ \ 1$

$a^{171} = -1\ \ 0\ \ 0$

$a^{172} = 0\ -1\ \ 0$

$a^{173} = 0\ \ 0\ -1$

$a^{174} = 2\ \ 2\ \ 3$

$a^{175} = 1\ \ 3\ \ 0$

$a^{176} = 0\ \ 1\ \ 3$

$a^{270} = 1\ -1\ -2$

$a^{271} = -3\ -2\ -2$

$a^{272} = -3\ \ 1\ -3$

$a^{273} = -1\ \ 3\ \ 3$

$a^{274} = 1\ \ 0\ \ 1$

$a^{275} = -2\ -1\ -3$

$a^{276} = -1\ -3\ \ 1$

$a^{277} = -2\ -3\ \ 1$

$a^{278} = -2\ \ 3\ \ 1$

$a^{279} = -2\ \ 3\ \ 0$

$a^{280} = 0\ -2\ \ 3$

$a^{281} = 1\ \ 1\ \ 3$

$a^{282} = 1\ -2\ -1$

$a^{283} = 2\ \ 3\ -2$

$a^{284} = -3\ -1\ \ 2$

$a^{285} = 3\ \ 0\ \ 0$

$a^{286} = 0\ \ 3\ \ 0$

$a^{287} = 0\ \ 0\ \ 3$

$a^{288} = 1\ \ 1\ -2$

$a^{289} = -3\ -2\ \ 0$

$a^{290} = 0\ -3\ -2$

$a^{63} = 2\ 2\ -2$

$a^{64} = -3\ -1\ 1$

$a^{65} = -2\ 2\ 3$

$a^{66} = 1\ -1\ 0$

$a^{67} = 0\ 1\ -1$

$a^{68} = 2\ 2\ -3$

$a^{69} = -1\ 1\ -3$

$a^{70} = -1\ -2\ 3$

$a^{71} = 1\ 0\ 3$

$a^{72} = 1\ 2\ -2$

$a^{73} = -3\ -2\ 1$

$a^{74} = -2\ 2\ 2$

$a^{75} = 3\ 1\ 3$

$a^{76} = 1\ -3\ -1$

$a^{77} = 2\ 3\ 0$

$a^{78} = 0\ 2\ 3$

$a^{79} = 1\ 1\ 0$

$a^{80} = 0\ 1\ 1$

$a^{81} = -2\ -2\ -2$

$a^{82} = -3\ +2\ -3$

$a^{83} = -1\ 3\ -3$

$a^{177} = 1\ 1\ -1$

$a^{178} = 2\ 3\ -3$

$a^{179} = -1\ 1\ -2$

$a^{180} = -3\ 3\ 0$

$a^{181} = 0\ -3\ 3$

$a^{182} = 1\ 1\ 2$

$a^{183} = 3\ -3\ 2$

$a^{184} = 3\ -1\ -2$

$a^{185} = -3\ 0\ -2$

$a^{186} = -3\ 1\ -1$

$a^{187} = 2\ -1\ -3$

$a^{188} = -1\ 1\ 1$

$a^{189} = -2\ -3\ -2$

$a^{190} = -3\ 2\ 3$

$a^{191} = 1\ -2\ 0$

$a^{192} = 0\ 1\ -2$

$a^{193} = -3\ -3\ 0$

$a^{194} = 0\ -3\ -3$

$a^{195} = -1\ -1\ -1$

$a^{196} = 2\ 1\ 2$

$a^{197} = 3\ -2\ 2$

$a^{291} = -3\ -3\ 3$

$a^{292} = 1\ -2\ 2$

$a^{293} = 3\ -3\ -1$

$a^{294} = 2\ -2\ 0$

$a^{295} = 0\ 2\ -2$

$a^{296} = -3\ -3\ 1$

$a^{297} = -2\ 2\ 1$

$a^{298} = -2\ 3\ -1$

$a^{299} = 2\ 0\ -1$

$a^{300} = 2\ -3\ 2$

$a^{301} = 1\ 3\ 2$

$a^{302} = 3\ -3\ -3$

$a^{303} = -1\ 2\ -1$

$a^{304} = 2\ 1\ -2$

$a^{305} = -3\ -1\ 0$

$a^{306} = 0\ -3\ -1$

$a^{307} = 2\ -2\ 0$

$a^{308} = 0\ 2\ 2$

$a^{309} = 3\ 3\ 3$

$a^{310} = 1\ -3\ 1$

$a^{311} = -2\ -1\ 1$

$a^{84} = -1 \quad -2 \quad -2$

$a^{85} = -3 \quad 3 \quad -3$

$a^{86} = -1 \quad 3 \quad -2$

$a^{87} = -3 \quad 3 \quad 2$

$a^{88} = 3 \quad 0 \quad -3$

$a^{89} = -1 \quad 2 \quad 2$

$a^{90} = 3 \quad 2 \quad 3$

$a^{91} = 1 \quad -3 \quad 0$

$a^{92} = 0 \quad 1 \quad -3$

$a^{93} = -1 \quad -1 \quad 3$

$a^{94} = 1 \quad 0 \quad -3$

$a^{95} = -1 \quad 0 \quad 2$

$a^{96} = 3 \quad 2 \quad 1$

$a^{97} = -2 \quad 1 \quad -1$

$a^{98} = 2 \quad 0 \quad -3$

$a^{99} = -1 \quad 1 \quad 2$

$a^{100} = 3 \quad 2 \quad 2$

$a^{101} = 3 \quad -1 \quad 3$

$a^{102} = 1 \quad -3 \quad -3$

$a^{103} = -1 \quad 0 \quad -1$

$a^{104} = 2 \quad 1 \quad 3$

$a^{198} = 3 \quad -1 \quad -1$

$a^{199} = 2 \quad -2 \quad 2$

$a^{200} = 3 \quad -2 \quad -1$

$a^{201} = 2 \quad -2 \quad 1$

$a^{202} = -2 \quad 0 \quad 2$

$a^{203} = 3 \quad 1 \quad 1$

$a^{204} = -2 \quad 1 \quad -2$

$a^{205} = -3 \quad 2 \quad 0$

$a^{206} = 0 \quad -3 \quad 2$

$a^{207} = 3 \quad 3 \quad -2$

$a^{208} = -3 \quad 0 \quad 2$

$a^{209} = 3 \quad 0 \quad 1$

$a^{210} = -2 \quad 1 \quad -3$

$a^{211} = -1 \quad -3 \quad 3$

$a^{212} = 1 \quad 0 \quad 2$

$a^{213} = 3 \quad -3 \quad 1$

$a^{214} = -2 \quad 1 \quad 1$

$a^{215} = -2 \quad 3 \quad -2$

$a^{216} = -3 \quad 2 \quad 2$

$a^{217} = 3 \quad 0 \quad 3$

$a^{218} = 1 \quad -3 \quad -2$

$a^{312} = -2 \quad 3 \quad 3$

$a^{313} = 1 \quad -1 \quad 1$

$a^{314} = -2 \quad -1 \quad 3$

$a^{315} = 1 \quad -1 \quad -3$

$a^{316} = -1 \quad 0 \quad -1$

$a^{317} = -2 \quad -3 \quad -3$

$a^{318} = -1 \quad -3 \quad -1$

$a^{319} = 2 \quad 1 \quad 0$

$a^{320} = 0 \quad 2 \quad 1$

$a^{321} = -2 \quad -2 \quad -1$

$a^{322} = 2 \quad 0 \quad 1$

$a^{323} = -2 \quad 0 \quad -3$

$a^{324} = -1 \quad -3 \quad 2$

$a^{325} = 3 \quad 2 \quad -2$

$a^{326} = -3 \quad 0 \quad 1$

$a^{327} = -2 \quad 2 \quad -3$

$a^{328} = -1 \quad -3 \quad -3$

$a^{329} = -1 \quad -2 \quad -1$

$a^{330} = 2 \quad 1 \quad 1$

$a^{331} = -2 \quad 0 \quad -2$

$a^{332} = -3 \quad 2 \quad -1$

$a^{105} = 1\ 3\ -1$	$a^{219} = -3\ -2\ 3$	$a^{333} = 2\ -1\ -2$
$a^{106} = 2\ 3\ -1$	$a^{220} = 1\ -2\ 3$	$a^{334} = -3\ -1\ -2$
$a^{107} = 2\ -3\ -1$	$a^{221} = 1\ 2\ 3$	$a^{335} = -3\ 1\ -2$
$a^{108} = 2\ -3\ 0$	$a^{222} = 1\ 2\ 0$	$a^{336} = -3\ 1\ 0$
$a^{109} = 0\ 2\ -3$	$a^{223} = 0\ 1\ 2$	$a^{337} = 0\ -3\ 1$
$a^{110} = -1\ -1\ -3$	$a^{224} = 3\ 3\ 2$	$a^{338} = -2\ -2\ 1$
$a^{111} = -1\ -2\ 1$	$a^{225} = -3\ -1\ -3$	$a^{339} = -2\ 3\ 2$
$a^{112} = -2\ -3\ 2$	$a^{226} = -1\ 2\ 1$	$a^{340} = 3\ 1\ -3$
$a^{113} = 3\ 1\ -2$	$a^{227} = -2\ -3\ -1$	$a^{341} = -1\ 2\ 3$

The corresponding generator polynomial is :

$$g(x) = 1 - x + 2x^3 + x^4 - 2x^5 - 3x^6 + 2x^7 + 2x^8 + x^9$$

A-5.

For $p = 11$, $r = 2$ then $t = 5$ and $n = 60$.

$1 + x^{60} =$	Irreducible polynomials	Root order
	$(-5\ -3x + x^2)$	120*
	$(-5,\ -2,\ 1)$	120*
	$(-5,\ -1,\ 1)$	40
	$(-5,\ 1,\ 1)$	40
	$(-5,\ 2,\ 1)$	120*
	$(-5,\ 3,\ 1)$	120*
	$(-4,\ -5,\ 1)$	40
	$(-4,\ -4,\ 1)$	120*
	$(-4,\ -1,\ 1)$	120*
	$(-4,\ 1,\ 1)$	120*
	$(-4,\ 4,\ 1)$	120*
	$(-4,\ 5,\ 1)$	40
	$(-3,\ -4,\ 1)$	40
	$(-3,\ -3,\ 1)$	120*
	$(-3,\ -1,\ 1)$	120*
	$(-3,\ 1,\ 1)$	120*
	$(-3,\ 3,\ 1)$	120*
	$(-3,\ 4,\ 1)$	40

(-1, -5, 1)	24
(-1, -3, 1)	8
(-1, -2, 1)	24
(-1, 2, 1)	24
(-1, 3, 1)	8
(-1, 5, 1)	24
(2, -5, 1)	120*
(2, -4, 1)	120*
(2, -2, 1)	40
(2, 2, 1)	40
(2, 4, 1)	120*
(2, 5, 1)	120

* indicates the corresponding polynomial is primitive .

GF (11^2) in terms of α, a root of $-5 - 3x + x^2$

$\alpha^0 = 1$	$\alpha^{40} = -5\ 3$	$\alpha^{80} = 4\ -3$
$\alpha^1 = 1$	$\alpha^{41} = 4\ 4$	$\alpha^{81} = -4\ -5$
$\alpha^2 = 5\ 3$	$\alpha^{42} = -2\ 5$	$\alpha^{82} = -3\ 3$
$\alpha^3 = 4\ 3$	$\alpha^{43} = 3\ 2$	$\alpha^{83} = 4\ -5$
$\alpha^4 = 4\ 2$	$\alpha^{44} = -1\ -2$	$\alpha^{84} = -3\ 0$
$\alpha^5 = -1\ -1$	$\alpha^{45} = 1\ 4$	$\alpha^{85} = 0\ -3$
$\alpha^6 = -5\ -4$	$\alpha^{46} = -2\ 2$	$\alpha^{86} = -4\ 2$
$\alpha^7 = 2\ 5$	$\alpha^{47} = -1\ 4$	$\alpha^{87} = -1\ 2$
$\alpha^8 = 3\ -5$	$\alpha^{48} = -2\ 0$	$\alpha^{88} = -1\ -5$
$\alpha^9 = -3\ -1$	$\alpha^{49} = 0\ -2$	$\alpha^{89} = 3\ 3$
$\alpha^{10} = -5\ 5$	$\alpha^{50} = 1\ 5$	$\alpha^{90} = 4\ 1$
$\alpha^{11} = 3\ -1$	$\alpha^{51} = 3\ 5$	$\alpha^{91} = 5\ -4$
$\alpha^{12} = -5\ 0$	$\alpha^{52} = 3\ -4$	$\alpha^{92} = -2\ 4$
$\alpha^{13} = 0\ -5$	$\alpha^{53} = 2\ 2$	$\alpha^{93} = -2\ 3$
$\alpha^{14} = -3\ -4$	$\alpha^{54} = -1\ -3$	$\alpha^{94} = 4\ -4$
$\alpha^{15} = 2\ -4$	$\alpha^{55} = -4\ 1$	$\alpha^{95} = 2\ 3$
$\alpha^{16} = 2\ 1$	$\alpha^{56} = 5\ -1$	$\alpha^{96} = 4\ 0$
$\alpha^{17} = 5\ 5$	$\alpha^{57} = -5\ 2$	$\alpha^{97} = 0\ 4$
$\alpha^{18} = 3\ -2$	$\alpha^{58} = -1\ 1$	$\alpha^{98} = -2\ 1$
$\alpha^{19} = 1\ -3$	$\alpha^{59} = 5\ 2$	$\alpha^{99} = 5\ 1$

$a^{20} = -4\ \ 3$
$a^{21} = 4\ \ 5$
$a^{22} = 3\ \ -3$
$a^{23} = -4\ \ 5$
$a^{24} = 3\ \ 0$
$a^{25} = 0\ \ 3$
$a^{26} = 4\ \ -2$
$a^{27} = 1\ \ -2$
$a^{28} = 1\ \ -5$
$a^{29} = -3\ \ -3$
$a^{30} = -4\ \ -1$
$a^{31} = -5\ \ 4$
$a^{32} = -2\ \ -4$
$a^{33} = 2\ \ -3$
$a^{34} = -4\ \ 4$
$a^{35} = -2\ \ -3$
$a^{36} = -4\ \ 0$
$a^{37} = 0\ \ -4$
$a^{38} = 2\ \ -1$
$a^{39} = -5\ \ -1$

$a^{60} = -1$
$a^{61} = 0\ \ -1$
$a^{62} = -5\ \ -3$
$a^{63} = -4\ \ -3$
$a^{64} = -4\ \ -2$
$a^{65} = 1\ \ 1$
$a^{66} = 5\ \ 4$
$a^{67} = -2\ \ -5$
$a^{68} = -3\ \ 5$
$a^{69} = 3\ \ 1$
$a^{70} = 5\ \ -5$
$a^{71} = -3\ \ 1$
$a^{72} = 5\ \ 0$
$a^{73} = 0\ \ 5$
$a^{74} = 3\ \ 4$
$a^{75} = -2\ \ 4$
$a^{76} = -2\ \ -1$
$a^{77} = -5\ \ -5$
$a^{78} = -3\ \ 2$
$a^{79} = -1\ \ 3$

$a^{100} = 5\ \ -3$
$a^{101} = -4\ \ -4$
$a^{102} = 2\ \ -5$
$a^{103} = -3\ \ -2$
$a^{104} = 1\ \ 2$
$a^{105} = -1\ \ -4$
$a^{106} = 2\ \ -2$
$a^{107} = 1\ \ -4$
$a^{108} = 2\ \ 0$
$a^{109} = 0\ \ 2$
$a^{110} = -1\ \ -5$
$a^{111} = -3\ \ -5$
$a^{112} = -3\ \ 4$
$a^{113} = -2\ \ -2$
$a^{114} = 1\ \ 3$
$a^{115} = 4\ \ -1$
$a^{116} = -5\ \ 1$
$a^{117} = 5\ \ -2$
$a^{118} = 1\ \ -1$
$a^{119} = -5\ \ -2$

The corresponding generator polynomial is :

$$g(x) = -1 - 5x + 5x^2 - 3x^4 + x^5 + 5x^6 - 4x^8 - 3x^9 + x^{10}$$

A-6.

For $p = 13$, $r = 2$ then $t = 6$ and $n = 84$.

$1 + x^{84} =$	Irreducible polynomials	Root order
	$(-6 - 6x + x^2)$	168*
	$(-6, -3, 1)$	168*
	$(-6, -2, 1)$	168*
	$(-6, 0, 1)$	24
	$(-6, 2, 1)$	168*
	$(-6, 3, 1)$	168*
	$(-6, 6, 1)$	168*
	$(-5, -5, 1)$	56
	$(-5, -2, 1)$	56
	$(-5, -1, 1)$	56
	$(-5, 0, 1)$	8
	$(-5, 1, 1)$	56
	$(-5, 2, 1)$	56
	$(-5, 5, 1)$	56
	$(-2, -6, 1)$	168*
	$(-2, -5, 1)$	168*
	$(-2, -4, 1)$	168*
	$(-2, 0, 1)$	24

(-2 , 4 , 1)	168*
(-2 , 5 , 1)	168*
(-2 , 6 , 1)	168*
(2 , -6 , 1)	168*
(2 , -4 , 1)	168*
(2 , -1 , 1)	168*
(2 , 0 , 1)	24
(2 , 1 , 1)	168*
(2 , 4 , 1)	168*
(2 , 6 , 1)	168*
(5 , -5 , 1)	56
(5 , -3 , 1)	56
(5 , 3 , 1)	56
(5 , -1 , 1)	56
(5 , 0 , 1)	8
(5 , 1 , 1)	56
(5 , 5 , 1)	56
(6 , -4 , 1)	168*
(6 , -3 , 1)	168*
(6 , -2 , 1)	168*
(6 , 0 , 1)	24

(6 , 2 , 1)	168*
(6 , 3 , 1)	168*
(6 , 4 , 1)	168*

*indicates the corresponding polynomial is primitive.

GF(x) in terms of α, a root of $-6 - 6x + x^2$.

$\alpha^0 = 1$	$\alpha^{56} = -4 \quad 0$	$\alpha^{112} = 3 \quad 0$
$\alpha^1 = 0 \quad 1$	$\alpha^{57} = 0 \quad -4$	$\alpha^{113} = 0 \quad 3$
$\alpha^2 = 6 \quad 6$	$\alpha^{58} = 2 \quad 2$	$\alpha^{114} = 5 \quad 5$
$\alpha^3 = -3 \quad 3$	$\alpha^{59} = -1 \quad 1$	$\alpha^{115} = 4 \quad -4$
$\alpha^4 = 5 \quad 2$	$\alpha^{60} = 6 \quad 5$	$\alpha^{116} = 2 \quad 6$
$\alpha^5 = -1 \quad 4$	$\alpha^{61} = 4 \quad -3$	$\alpha^{117} = -3 \quad -1$
$\alpha^6 = -2 \quad -1$	$\alpha^{62} = -5 \quad -1$	$\alpha^{118} = -6 \quad 4$
$\alpha^7 = -5 \quad 6$	$\alpha^{63} = -6 \quad 2$	$\alpha^{119} = -2 \quad 5$
$\alpha^8 = -3 \quad 5$	$\alpha^{64} = -1 \quad 6$	$\alpha^{120} = 4 \quad 2$
$\alpha^9 = 4 \quad 1$	$\alpha^{65} = -3 \quad -4$	$\alpha^{121} = -1 \quad 3$
$\alpha^{10} = 6 \quad -3$	$\alpha^{66} = 2 \quad -1$	$\alpha^{122} = 5 \quad 4$
$\alpha^{11} = -5 \quad 1$	$\alpha^{67} = -6 \quad -4$	$\alpha^{123} = 3 \quad -2$
$\alpha^{12} = 6 \quad 1$	$\alpha^{68} = 2 \quad -4$	$\alpha^{124} = 5 \quad 3$
$\alpha^{13} = 6 \quad -1$	$\alpha^{69} = 2 \quad 4$	$\alpha^{125} = 5 \quad -3$

$a^{14} = -6 \quad 0$

$a^{15} = 0 \quad -6$

$a^{16} = 3 \quad 3$

$a^{17} = 5 \quad -5$

$a^{18} = -4 \quad 1$

$a^{19} = 6 \quad 2$

$a^{20} = -1 \quad 5$

$a^{21} = 4 \quad 3$

$a^{22} = 5 \quad -4$

$a^{23} = 2 \quad -6$

$a^{24} = 3 \quad 5$

$a^{25} = 4 \quad -6$

$a^{26} = 3 \quad -6$

$a^{27} = 3 \quad 6$

$a^{28} = -3 \quad 0$

$a^{29} = 0 \quad -3$

$a^{30} = -5 \quad -5$

$a^{31} = -4 \quad 4$

$a^{32} = -2 \quad -6$

$a^{33} = 3 \quad 1$

$a^{34} = 6 \quad -4$

$a^{70} = -2 \quad 0$

$a^{71} = 0 \quad -2$

$a^{72} = 1 \quad 1$

$a^{73} = 6 \quad -6$

$a^{74} = 3 \quad -4$

$a^{75} = 2 \quad 5$

$a^{76} = 4 \quad 6$

$a^{77} = -3 \quad 1$

$a^{78} = 6 \quad 3$

$a^{79} = 5 \quad -2$

$a^{80} = 1 \quad 6$

$a^{81} = -3 \quad -2$

$a^{82} = 1 \quad -2$

$a^{83} = 1 \quad 2$

$a^{84} = -1 \quad 0$

$a^{85} = 0 \quad -1$

$a^{86} = -6 \quad -6$

$a^{87} = 3 \quad -3$

$a^{88} = -5 \quad -2$

$a^{89} = 1 \quad -4$

$a^{90} = 2 \quad 1$

$a^{126} = -5 \quad 0$

$a^{127} = 0 \quad -5$

$a^{128} = -4 \quad -4$

$a^{129} = 2 \quad -2$

$a^{130} = 1 \quad 3$

$a^{131} = 5 \quad 6$

$a^{132} = -3 \quad 2$

$a^{133} = -1 \quad -4$

$a^{134} = 2 \quad 1$

$a^{135} = 6 \quad -5$

$a^{136} = -4 \quad 2$

$a^{137} = -1 \quad -5$

$a^{138} = -4 \quad -5$

$a^{139} = -4 \quad 5$

$a^{140} = 4 \quad 0$

$a^{141} = 0 \quad 4$

$a^{142} = -2 \quad -2$

$a^{143} = 1 \quad -1$

$a^{144} = -6 \quad -5$

$a^{145} = -4 \quad 3$

$a^{146} = 5 \quad 1$

$a^{35} = 2\ -5$
$a^{36} = -4\ -2$
$a^{37} = 1\ -3$
$a^{38} = -5\ -4$
$a^{39} = 2\ -3$
$a^{40} = -5\ -3$
$a^{41} = -5\ 3$
$a^{42} = 5\ 0$
$a^{43} = 0\ 5$
$a^{44} = 4\ 4$
$a^{45} = -2\ 2$
$a^{46} = -1\ -3$
$a^{47} = -5\ -6$
$a^{48} = 3\ -2$
$a^{49} = 1\ 4$
$a^{50} = -2\ -1$
$a^{51} = -6\ 5$
$a^{52} = 4\ -2$
$a^{53} = 1\ 5$
$a^{54} = 4\ 5$
$a^{55} = 4\ -5$

$a^{91} = 5\ -6$
$a^{92} = 3\ -5$
$a^{93} = -4\ -1$
$a^{94} = -6\ 3$
$a^{95} = 5\ -1$
$a^{96} = -6\ -1$
$a^{97} = -6\ 1$
$a^{98} = 6\ 0$
$a^{99} = 0\ 6$
$a^{100} = -3\ -3$
$a^{101} = 5\ 5$
$a^{102} = 4\ -1$
$a^{103} = -6\ -2$
$a^{104} = 1\ -5$
$a^{105} = -4\ -3$
$a^{106} = -5\ 4$
$a^{107} = -2\ 6$
$a^{108} = -3\ -5$
$a^{109} = -4\ 6$
$a^{110} = -3\ 6$
$a^{111} = -3\ -6$

$a^{147} = 6\ -2$
$a^{148} = 1\ -6$
$a^{149} = 3\ 4$
$a^{150} = -2\ 1$
$a^{151} = 6\ 4$
$a^{152} = -2\ 4$
$a^{153} = -2\ -4$
$a^{154} = 2\ 0$
$a^{155} = 0\ 2$
$a^{156} = -1\ -1$
$a^{157} = -6\ 6$
$a^{158} = -3\ 4$
$a^{159} = -2\ -5$
$a^{160} = -4\ -6$
$a^{161} = 3\ -1$
$a^{162} = -6\ 3$
$a^{163} = -5\ 2$
$a^{164} = -1\ -6$
$a^{165} = 3\ 2$
$a^{166} = -1\ 2$
$a^{167} = -1\ -2$

The corresponding generator polynomial is :

$$g(x) = 1 + 4x - 2x^2 + 5x^3 + 4x^4 - 2x^5 + 4x^7 - 3x^8 - x^9 + 6x^{10} + 2x^{11} + x^{12}$$

APPENDIX B

oOo

In Appendix A , the block lengths of the codes given are $\nu = p^r - 1$. In this Appendix , the codes considered have block lengths n , which are fractions of $p^2 - 1$. That means, for each prime p , we have

$$\nu = \frac{p^2 - 1}{2} = nc ,$$

where

n is the considered block length ,

c is an odd integer .

p	n	t	Primitive polynomial	Generator polynomial
5	12	2	$-2 - 2x + x^2$	$1 + x - 2x^3 + x^4$
	4	1	-id-	$-2 + x^2$
	12	2	$-2 + 2x + x^2$	$1 - x + 2x^3 + x^4$
	4	1	-id-	$2 + x^2$
7	24	3	$3 - x + x^2$	$-1 + x - 3x^2 + x^3 - x^4 - 3x^5 + x^6$
	8	3	-id-	$1 + 2x + 2x^2 - 2x^3 + x^4$
	8	1	-id-	$-1 + x + x^2$
11	60	5	$-5 - 3x + x^2$	$-1 - 5x + 5x^2 - 3x^4 + x^5 + 5x^6 - 4x^8 - 3x^9 + x^{10}$
	20	5	-id-	$-1 - 2x - 2x^2 + 5x^3 + x^4 + 3x^5 - 3x^6 + x^7 - x^8 - 3x^9 + x^{10}$
	20	4	"	$4 - 5x - x^2 - x^3 - 2x^4 - 4x^5 - 5x^6 - x^7 + x^8$
	20	3	"	$-3 - 5x + 5x^2 - 4x^3 + x^6$
	20	2	"	$3 - 4x + x^2 + 3x^3 + x^4$
	20	1	"	$-4 + 5x + x^2$
	12	5	"	$-1 + 4x + 3x^2 - 5x^3 - 3x^4 + 4x^5 + x^6$
	12	2	"	$1 - 2x + 5x^2 + 2x^3 + x^4$
	12	1	"	$-1 + 5x + x^2$
	4	1	"	$-1 - 3x + x^2$

REFERENCES.

1. Howard Falk, " Convolutional coding arrives ", IEEE Spectrum, January 1974, pp. 35-36.

2. Chien, R.T., " Memory error control : beyond parity ", IEEE Spectrum, July 1973, pp. 18-23.

3. W.Wesley Peterson; E.J. Weldon,Jr., Error-correcting codes. Second edition, The MIT Press, Massachusetts, 1972.

4. ————————, pp. 19-38 and 144-168.

5. ————————, chapter 12.

6. Elwyn R. Berlekamp, Algebraic coding theory. McGraw Hill, 1968, pp. 207-217.

7. ————————, page 204.

8. ————————, page 213.

9. R.C. Bose and T.A. Dowling, "Combinatorial mathematics and its applications ", Proceedings of the Conference at the University of North Carolina, North Carolina, pp. 298-315 (April 10-14 1967).

10. Jessie Macwilliams, " Permutation decoding of systematic codes ", The Bell System Technical Journal, January 1964, pp. 485-505.

11. Birkhoff, G; S. MacLane, 1941, A survey of modern algebra, New York : The Macmillan Co.

12. Shu Lin., An introduction to Error-correcting codes, Prentice-Hall, 1970, chapter 7.