THE WEIGHT DISTRIBUTION OF SOME QUASI-CYCLIC CODES

CAT NGUYEN

A Master Thesis

in

The Department

of

Electrical Engineering

October 1979

Concordia University

Presented in Partial Fulfillment of the Requirements
for the degree of Master of Engineering at
Concordia University
Montréal, Québec, Canada

© Cat Nguyen, 1979

ABSTRACT

The Weight Distribution of Some Quasi-Cyclic Codes

Cat Nguyen

In this thesis, the weight distribution and the decoding problem of quasi-cyclic codes are studied.

Weight distributions of quasi-cyclic codes (some known and some new) are computed and analyzed. Quasi-cyclic codes of rate 1/3, 1/2 and 2/3 are studied in detail.

The Karlin binary decoder is optimized with channel measurement information.

The class of quasi-cyclic codes derived from power residue codes, with the normal basis theorem, are found to generate very good sub-codes which are comparable to the best codes listed in McWilliams & Sloane.

Finally, some quasi-cyclic codes are found to have very good weight distribution structures which are well-suited for expurgation to form constant weight codes.

ACKNOWLEDGEMENTS

I wish to express my sincere gratitude to Dr V.K.Bhargava, for his helpful suggestions, counsel and encouragement.

Special thanks should go to Miss Phoung Lan for her helps in computer programs.

I wish to extend my thanks to Miss Elisa Morrell for English correction and my sister, Miss Hang Nguyen for typing the complete manuscript.

TABLE OF CONTENTS

LIST OF ABBREVIATION

(n,k)	A linear code of length n and k information symbols
d, d_{min}	minimum distance of the code
A_i	Number of codeword of weight i in a code
G	generator matrix
C	circulant matrix
$C(x)$	polynomial associated with C
$GF(2)$	Galois field of 2 elements 0 and 1
C^T	transposed matrix of matrix C
$R = \frac{k}{n}$	rate of the code

CHAPTER 1

1.1 Introduction In this chapter, we introduce some known mathematical notions necessary to the development of the thesis. The reader is assumed to be familiar with the notion of Galois field.

The factorization of x^n-1 is reviewed first and the problem of how many polynomials $f_n(x)$ of degree n, n odd integer, such that GCD $\left(f_n(x), x^n-1\right)$ is considered.

Since the problem of determining m^{th} power residues is a generalization of determining quadratic residues, the notion of quadratic congruence is also reviewed.

Finally the well-known isomorphism property between the algebra of circulant matrices and polynomials mod x^n-1 over GF(2) is demonstrated.

1.2 Factorization of x^n-1 over GF(2)

Our main concern here is about the factorization of x^n-1, n odd integer, over GF(2) where the roots of x^n-1 lie in the $GF(2^m)$. Since 2 and n are relatively prime, there will be at least an integer m such that $2^m \equiv 1 \pmod{n}$.

In the field $GF(2^m)$, (x^n-1) can be factorized into

$$x^n-1 = (x-\alpha^0)(x-\alpha^1)(x-\alpha^2)\ldots(x-\alpha^{n-1}) \quad (1.1)$$

Let us define the minimal polynomial $M_i(x)$ such that

$$M_i(x) = (x-\beta_1)(x-\beta_2)\ldots(x-\beta_r) \quad (1.2)$$

where $\beta_1, \beta_2, \ldots, \beta_r$ are all elements belonging to the same cyclotomic coset mod x^n-1.

To visualize, the cyclotomic coset mod 3,7,23,31,63,127 are

Mod 3

$C_0 = \{0\}$

$C_1 = \{1,2\}$

mod 7

$C_0 = \{0\}$

$C_1 = \{1,2,4\}$

$C_3 = \{3,6,5\}$

mod 23

$C_0 = \{0\}$

$C_1 = \{1,2,4,8,16,9,18,13,3,6,12\}$

$C_5 = \{5,10,20,17,11,22,21,19,15,7,14\}$

mod 31

$C_0 = \{0\}$

$C_1 = \{1,2,4,8,16\}$

$C_3 = \{3,6,12,24,17\}$

$C_5 = \{5,10,20,9,18\}$

$C_7 = \{7,14,28,25,19\}$

$C_{11} = \{11,22,13,26,21\}$

$C_{15} = \{15,30,29,27,23\}$

mod 63

$C_0 = \{0\}$
$C_1 = \{1,2,4,8,16,32\}$
$C_3 = \{3,6,12,24,48,33\}$
$C_5 = \{5,10,20,40,17,34\}$
$C_7 = \{7,14,28,56,49,35\}$
$C_9 = \{9,18,36\}$
$C_{11} = \{11,22,44,25,50,37\}$
$C_{13} = \{13,26,52,41,19,38\}$
$C_{15} = \{15,30,60,57,51,39\}$
$C_{21} = \{21,42\}$
$C_{23} = \{23,46,29,58,53,43\}$
$C_{27} = \{27,54,45\}$
$C_{31} = \{31,62,61,59,55,47\}$

mod 127

$C_0 = \{0\}$
$C_1 = \{1,2,4,8,16,32,64\}$
$C_3 = \{3,6,12,24,48,96,65\}$
$C_5 = \{5,10,20,40,80,33,66\}$
$C_7 = \{7,14,28,56,112,97,67\}$
$C_9 = \{9,18,36,72,17,34,68\}$
$C_{11} = \{11,22,44,88,49,98,69\}$
$C_{13} = \{13,26,52,104,81,35,70\}$
$C_{15} = \{15,30,60,120,113,99,71\}$
$C_{19} = \{19,38,76,25,50,100,73\}$
$C_{21} = \{21,42,84,41,82,37,74\}$
$C_{23} = \{23,46,92,57,114,101,75\}$
$C_{27} = \{27,54,108,89,51,102,75\}$
$C_{29} = \{29,58,116,105,83,39,78\}$
$C_{31} = \{31,62,124,121,115,103,79\}$
$C_{43} = \{43,86,45,90,53,106,85\}$
$C_{47} = \{47,94,61,122,117,107,87\}$
$C_{55} = \{55,110,93,59,118,109,91\}$
$C_{63} = \{63,126,125,123,119,111,95\}$

Then x^n-1 can be factorized into minimal polynomials as

$$x^n-1 = M_0(x).M_1(x)...M_s(x) \qquad (1.3)$$

$$s = (n-1)/2$$

Equivalently

$$x^n-1 = \prod_s M_s(x) \qquad (1.4)$$

where s runs through the coset representatives mod 2^n-1

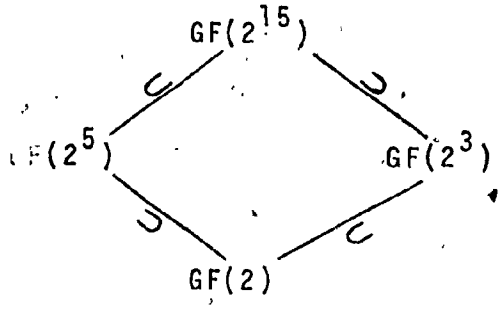
Therefore we can have the following theorem.

Theorem 1.2.1 Let R_m be the ensemble of monic polynomials $M_i(x)$ irreducible over GF(2), whose product divides x^n-1, n odd integer. Then there are at least $1/2\ 2^m$ elements of R_m having degree m and do not belong to any other subfield.

Proof Let $M_i(x)$ be an element of R_m and having degree v less than m. Then the roots of $M_i(x)$ belong to a field $GF(2^d)$ a subfield of $GF(2^m)$.

There are at least 2^{m-1} elements of R_m which do not belong to any other field.

This can be visualized as in fig. 1.1 for two specific cases.



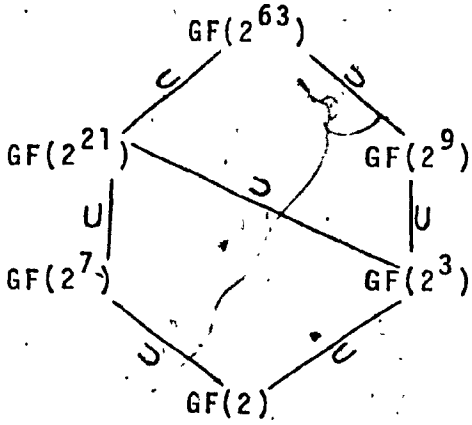


Fig. 1.1 Subfields of $GF(2^{15})$ and $GF(2^{63})$

Fig 1.2 gives the factors of x^n-1 over GF(2) for n odd integer, n =33

n	Factors (in Octal)
3	6.7
7	6.54.64
9	6.7.444
11	6.7771
13	6.7773
15	6.7.46.62.76
17	6.471.727
19	6.777777
21	6.7.54.64.534.724
23	6.5343.6165
25	6.76.5102041
27	6.7.444.4004004
29	6.77777771
31	6.45.51.57.67.73.75
33	6.7.4522.6106.7776

Fig 1.2 Factors of x^n-1 over GF(2), the factors are given in octal with the lowest degree terms in the left.

Our main question now is: How many polynomials $f_i(x)$ of degree n, n odd integer, such that

$$\text{GCD}\left[f_i(x),\ x^n-1\right] = 1 \qquad (1.5)$$

Let R_m be the ensemble of monic polynomials $M_i(x)$ irreducible over GF(2). Then equation (1.5) is equivalent to

$$\text{GCD}\left[f_i(x),\{M_i(x)\mid M_i(x)\in R_m\}\right] = 1 \qquad (1.6)$$

Let us consider now the case n odd integer and relatively large (as it should be on any asymptotic bound).
$M_1(x) = x+1$ (listed 6 in octal in fig 1.2)
divides all even polynomials of degree n.
$M_i(x)$ of degree i will divide 2^{n-1} polynomials of degree n where about half are odd and half are even, the later are also divisible by $M_1(x)$. All minimal polynomials of degree i divide the same polynomials.

For example, for $n = 3$, $M_1(x) = x+1$ divides $2^{3-1} = 4$ polynomials of degree 3, $M_2(x) = x^2+x+1$ divides $2^{3-2} = 2$ polynomials of degree 3 where one is also divisible by $M_1(x)$. Therefore, the number of polynomials $f_i(x)$ of degree 3 such that GCD $[f_i(x), x^3-1] = 1$ is exactly 3.

Similarly, for $n = 23$, $M_1(x) = x+1$ divides 2^{22} polynomials of degree 23.

$$M_2(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$$

and $$M_3(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + x^1$$

divides 2^{12} polynomials of degree 23, where about half are odd and half are even. Therefore, the number of polynomials $f_i(x)$ of degree 23 such that GCD $[f_i(x), x^{23}-1] = 1$ is about

$$2^{23} - (2^{22} + \frac{1}{2}\,12)$$

Therefore, in the limit (of the worst case) the number of polynomials $f_i(x)$ of degree n such that GCD $[f_i(x), x^n-1] = 1$ is bounded by :

$$2^n - 2^{n-1} - \frac{1}{2}\,2^{n-2} - \ldots - \frac{1}{2^{n-2}}\,2^{n-2} \qquad (1.7)$$

as $m \to \infty$

Eq (1.7) is equal to $\frac{1}{4}\,2^n$.

Thus we have demonstrated the well known result, that the number of polynomials $f_n(x)$ of degree n, n odd integer and relatively large, such that GCD $[f_n(x), x^n-1] = 1$ is lower bounded by 2^{n-2} and the polynomials are all distinct.

1.3 The notion of quadratic congruence

Let p be an odd prime with $(n,p)=1$. Then we have the following definition of the notion of quadratic congruence.

Definition 1.3.1 n is called a quadratic residue module p if and only of $x^2 \equiv n \pmod p$ has a solution.

The following notation, due to Legendre, is very useful in the study of quadratic residues.

Definition 1.3.2 Let p be an odd prime and $(n,p) = 1$. Then the Legendre symbol is defined as:

$(\frac{n}{p}) = 1$ if n is a quadratic residue mod p

$= -1$ is n is a quadratic non residue mod p

In terms of the legendre symbol, $(\frac{1}{7}) = (\frac{2}{7}) = (\frac{4}{7}) = 1$ $(\frac{3}{7}) = (\frac{5}{7}) = (\frac{6}{7}) = -1$ and $(\frac{a^2}{p}) = 1$ for any odd prime p, provided $(a,p) = 1$.

Theorem 1.3.3 Let p be an odd prime with $(n,p) = (m,P) = 1$ If $n \equiv m \pmod p$, then $(\frac{n}{p}) = (\frac{m}{p})$.

Proof: If $n \equiv m \pmod p$, then $x^2 \equiv n \pmod p$ is solvable if and only if $x^2 \equiv m \pmod p$. Q.E.D.

Theorem 1.3.4 There are precisely $(p-1)/2$ incongruent quadratic residues modules p where p is an odd prime.

Proof: Since $x^2 \equiv y^2 \pmod p$ is $x \equiv y \pmod p$, those values of x in the reduced system $1,2,\ldots,p-1$ are considered.

Moreover, $(p-x)^2 \equiv x^2 \pmod p$ so that the squares of the numbers in the two sets $1,2,\ldots,(p-1)/2$ and $(p+1)/2,\ldots,p-1$ are congruent in pairs .

The squares $1^2,2^2,\ldots,(p-1)2/4$ are all incongruent mod p and any quadratic residue is congruent to one of the numbers $1^2,2^2,\ldots,(p-1)2/4$ Q.E.D

Following theorem of special interest is derived from the Quadratic Reprocity Law of Gauss (1)

Theorem 1.3.5 If p is an odd prime

$(\frac{2}{p}) = 1$ for $p \equiv \pm 1 \bmod 8$

$= -1$ for $p \equiv \pm 3 \bmod 8$

By Gauss's Lemma
$(\frac{2}{p}) = (-1)^r = (-1)^{(p^2-1)/8}$

Since p is odd, $p \equiv \pm 1$ or $p \equiv \pm 3 \pmod 8$
If $p \equiv \pm 1 \pmod 8$, then $p = \pm 1 + 8k$ for some integer k and:
$p^2 = 1 \pm 16k + 64k^2$
Therefore, $(p^2-1)/8$ is even and
$(\frac{2}{p}) = 1$
On the other hand, if $p \equiv \pm 3 \pmod 8$, then $p = \pm 3 + 8k$
for some integer k and:
$p^2 = 9 \pm 48k + 64k^2$
Therefore (p^2-1) is odd and
$(\frac{2}{p}) = -1$ Q.E.D

Therefore for p an odd prime of the form $8\mu \pm 1$, 2 is a quadratic residue modulo p and for p an odd prime of the form $8\mu \pm 3$, 2 is a quadratic nonresidue modulo p.

1.4 The isomorphism property between circulant matrices and polynomials (mod x^n-1) over GF(2)

It is known that the polynomials (mod x^n-1) with coefficients from GF(2) form a ring R_m.

Then we have to show that the circulants generated by polynomials mod (x^n-1) also form a ring M_n, and there is a one to one mapping from R_m to M_n.

First, let us define a circulant matrix of order n over GF(2).

$$A = \begin{bmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_{n-1} & a_0 & \dots & a_{n-2} \\ \dots & \dots & \dots & \dots \\ a_1 & a_2 & \dots & a_0 \end{bmatrix} \qquad (1.8)$$

with $a_i \in GF(2)$. Each row of the matrix is the previous one shifted once, the circulation is to the right.

Let f denote the mapping $f: M_n \to R_m$ defined by $f(x) = a(x)$

$a(x) = a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{m-1} \bmod (x^n-1)$

a(x) is formed by the leading row of circulant matrix A.

It can be easily verified that:

i) $f(A+B) = a(x) + b(x) \bmod (x^n-1)$ (1.9)

ii) $f(A.B) = a(x) \cdot b(x) \bmod (x^n-1)$ (1.10)

iii) $f(cA) = ca(x) \bmod (x^n-1)$ (1.11)

Therefore we have demonstrated again the well known fact that the algebra of all nxn circulant matrices over GF(2) is isomorphic to the algebra of all polynomials (mod x^n-1) over GF(2).

1.5 Definition of the quasi-cyclic codes

A code is called quasi-cyclic if there is some integer s such that every cyclic shift of a codeword by s places is again a codeword. Of course a cyclic code is a quasi-cyclic code with s = 1. (12). Therefore a (mk,k) quasi-cyclic code is composed of m circulants, s = k, and its generator matrix can be expressed as:

$$G = [C_1, C_2, \ldots, C_m] \qquad (1.12)$$

where C_i is a kxk circulant matrix, as defined in equation (1.8).

If any C_i is invertible, then the quasi-cyclic code can be expressed under systematic form as

$$G' = [I, C'_1, C'_2, \ldots, C'_{m-1}] \qquad (1.13)$$

where I is an identity matrix of order k and $C'_i = C_i x C^{-1}$ is a circulant matrix of order k.
Therefore every codeword of the code generated by the matrix G' of equation 1.13 is of the form.

$$V(x) = [i(x); i(x)C'_1(x), i(x)C'_2(x), \ldots, i(x)C'_{m-1}(x)]$$

Similarly a $(m(s+1), ms)$ rate $\frac{s}{s+1}$ quasi-cyclic code in the systematic form, is defined by its generator matrix G_s such that

$$G_s = \begin{bmatrix} I_{ms} & \begin{matrix} C_1 \\ C_2 \\ C_s \end{matrix} \end{bmatrix} \qquad (1.14)$$

where I_{ms} is an identity matrix of order ms and C_i is a circulant of order s. Each codeword of the matrix G_s of eq (1.14) can be expressed as:

$$V(x) = [i_1(x), i_2(x), \ldots, i_s(x); p(x)] \pmod{x^m-1} \quad (1.15)$$

where $p(x) = \sum_{j=1}^{s} i_j(x) C_j(x) \pmod{x^m-1}$

In this thesis, the weight distributions of quasi-cyclic codes are computed and analysed specifically for codes of rate 1/3, ½, 2/3. The Karlin binary decoder is also improved by channel measurement information. Also, quasi-cyclic codes are derived from power residue codes. Some of these subcodes are comparable to list codes listed in MacWilliams & Sloane. Finally, some quasi-cyclic codes, with very good weight distribution structure, are expurgated to form constant weight codes.

CHAPTER 2

The Weight distribution of Quasi-Cyclic codes

2.1 Introduction The weight distribution of a code contains the following information:

-The minimum distance of the code

-The weight distribution of its dual by way of McWilliams identities

-The probability of decoding errors and failures in the case of an incomplete decoding (2).

-The construction of expurgated codes which improve the random coding bound (4).

-The construction of constant weight codes as seen on chapter 5:

2.2 The minimum distance of Quasi-Cyclic codes.

Consider now a codeword $v(x)$ of a Quasi-Cyclic Code (mk,k); $v(x)$ can be expressed as:

$$v(x) = \left[i(x)C_1(x), i(x)C_2(x), i(x)C_3(x), \ldots, i(x)C_m(x)\right] \bmod (x^k-1) \quad (2.1)$$

For $i(x) = x^i$, then

$$v(x) = \left[x^iC_1(x), x^iC_2(x), x^iC_3(x), \ldots, x^iC_m(x)\right] \bmod (x^k-1) \quad (2.2)$$

and its weight is equal to

$$W\left[v(x)\right] = \left[W|x^iC_1(x)| + W|x^iC_2(x)| + W|x^iC_3(x)| + \ldots + W|x^iC_m(x)|\right] \quad (2.3)$$

For $x^i = 1$, then (2.3) becomes a simple upper bound on the minimum distance of a Quasi-Cyclic code (mk,k):

$$d_{min} \leq \left[W|C_1(x)| + W|C_2(x) + \ldots + W|C_m(x)|\right] \quad (2.4)$$

If the code is expressed in systematic form, expression (2.4) becomes:

$$d_{min} \leq \left[1 + W|C_1(x)| + \ldots + W|C_{m-1}(x)|\right] \quad (2.5)$$

Different computing methods are used to calculate the minimum distance of a (mk,k) Quasi-Cyclic codes.

The straightforward method of computing the minimum distance d is to find the weight of sums of i rows of G, for $i = 1,\ldots,d$. This requires examination of

$$\sum_{i=1}^{d} \binom{k}{i} \qquad (2.6)$$

codewords.

This method is inconvenient in that the code should be under systematic form.

Another method of interest is a refinement of the above one by Chen (5). Due to the quasi-cyclic nature of the code, the search can be terminated for the smallest value v_o of i such that

$$i = v_o > \{(d-1)k/n\}-1. \qquad (2.7)$$

If d_v is the weight of the codeword of minimum weight in the set given by $i = 1,2,\ldots,v$ where $v<v_o$. Then the upper and lower bound on d will be

$$d_v \geq d \geq \{(v+1)n/k\}+1 \qquad (2.8)$$

As an example the best (58,29) found up to date has a minimum distance at most 12 then the first mentioned method will require an examination of 122×10^6 codewords and the second method will require an examination of 2.2×10^6 codewords and the brute force method 536×10^6 codewords.

Rate	Circulants	d (Eq. 2.4)	d_{min}
(39,13)	C_1=1, C_2=14221, C_3=13556	15	12
(51,17)	C_1=1, C_2=214626, C_3=313151	18	16
(52,13)	C_1=1, C_2=7715, C_3=5477, C_4=2767	28	16
(91,13)	C_1=1, C_2=14221, C_3=17227 C_4=13006, C_5=14771, C_6=13556, C_7=10550	43	36
(150,15)	C_1=34175, C_2=1405, C_3=64272, C_4=21654, C_5=46517, C_6=56300, C_7=4272, C_8=20361, C_9=34132, C_{10}=44007.	59	59
(88,11)	C_1=1253, C_2=1467, C_3=2224, C_4=1355, C_5=1541, C_6=2547, C_7=2621, C_8=3145.	47	39
(30,5)	C_1=1, C_2=11, C_3=30, C_4=35, C_5=26, C_6=31	15	15
(30,15)	C_1=46517, C_2=34132	16	6
(30,15)	C_1=46517, C_2=20361	15	5
(30,15)	C_1=46517, C_2=4274	15	7

Table 2.1 Minimum distance bounds on some very good Quasi-Cyclic Codes.

2.3 The weight distribution fo the dual code $C^{\perp}$.

If C is a (n,k) linear code over GF(2), then its dual or orthogonal code $C^{\perp}$ is the set of vectors which are orthogonal to all codewords of C.

Hence

$C^{\perp} = \{u \mid u.v = 0, v \in C\}$

$C^{\perp}$ is exactly the set of all parity checks on C, $C^{\perp}$ is an (n,n-K) linear code. Therefore the weight distribution of the dual $C^{\perp}$ of a binary linear code C is uniquely determined by the weight enumerator of C. Based on this property, we have McWilliams theorem for binary linear codes (12).

Theorem 2.1 If C is an (n,k) binary linear code with dual code $C^{\perp}$, then

$$W_{C^{\perp}}(x,y) = \frac{1}{2^k} W_C(x+y, x-y) \qquad (2.10)$$

Equivalently;

$$\sum_{i=0}^{n} B_i x^{n-k} y^k = \frac{1}{2^k} \sum_{i=0}^{n} A_i (x+y)^{n-i} (x-y) \qquad (2.11)$$

$$\sum_{u \in C^{\perp}} x^{n-Wt(u)} y^{Wt(u)} = \frac{1}{2^k} \sum_{u \in C} (x+y)^{n-Wt(u)} (x-y)^{n-Wt(u)} \qquad (2.12)$$

where A_i denotes the number of codewords of weight i in C.

B_i denotes the number of codewords of weight i in $C^{\perp}$.

$$W_C(x,y) = \sum_{i=0}^{n} A_i x^{n-i} y^i = \sum_{u \in C} x^{n-Wt(u)} y^{Wt(u)}$$

$$W_{C^{\perp}}(x,y) = \sum_{i=0}^{n} B_i x^{n-i} y^i = \sum_{u \in C^{\perp}} x^{n-Wt(u)} y^{Wt(u)}$$

Let us consider the (30,5,15) code where the circulants and its weight distribution are given in chapter 4, then

$$W_C(x,y) = x^{30} + 16x^{15}y^{15} + 15x^{14}y^{16} \qquad (2.13)$$

$$W_C^{\perp}(x,y) = \frac{1}{32} W_C(x+y, x-y) \qquad (2.14)$$

$$= \frac{1}{32} \{(x+y)^{30} + 16(x+y)^{15}(x-y)^{15} + 15(x+y)^{14}(x-y)^{16}\}$$

Eq (2.14) is the expression of the weight distribution of the dual (30,25,d') code. This expression can be programmed on a digital computer to obtain the weight distribution of the dual code.

2.4 The weight distribution of rate 1/2 Quasi-Cyclic Code

Since the algebra of circulant matrices is isomorphic to the algebra of polynomials $C(x)$, every codeword in a systematic Quasi-Cyclic (2k,k) code can be represented as:

$$v(x) = [i(x), i(x)C(x)] \bmod x^k - 1 \qquad (2.15)$$

We will see that the structure of the weight distribution can be determined as following:

i) If $i(x) = 0$, then $i(x)C(x) = 0$, the all zero codeword appears in every code.

ii) If $i(x)$ is of even weight, then $i(x)C(x)$ is also of even weight independently of $C(x)$, therefore the weight of the n-tuple is even.

iii) If $i(x)$ is of odd weight, there are two possibilities. For $C(x)$ of odd weight, since $(x+1) \nmid i(x)C(x)$, then $i(x)C(x)$ is of odd weight, therefore the weight of the n tuples is even; For $C(x)$ of even weight, $i(x)C(x)$ is even, therefore the weight of the n-tuple is odd.

IV) If $i(x)$ is all one, there are two possibilities: For $C(x)$ of odd weight, $i(x)C(x)$ will be all one and the resulting n-tuple is an all-one codeword; for $C(x)$ of even weight, $i(x)C(x)$ will be all zero and the resulting n-tuple is an [1...1,0...0] codeword

Generalizing above discussions to non systematic (2k,k) Quasi-Cyclic codes, we can summarize.

i) The all zero codeword always appears.

ii) If $C_1(x)$ and $C_2(x)$ are odd-odd weight, then the all one codeword exists. Since the all-ones vector appears, so does the 1's complement of the n-tuple, therefore the weight distribution is symmetric.

The weight distribution of some (2k,k) codes with $C_1(x)$, $C_2(x)$ of odd weights and $C_1(x)$, $C_2(x)$ of different weights are given respectively in tables 2.2 and 2.3

$C_1(x)$	46517	46517	34175	34175	34175	21654	34175
$C_2(x)$	44007	34132	44007	46517	21654	46517	33132
0	1	1	1	1	1	1	1
1							
2							
3							
4							
5							
6	35	35	45	75	15	30	45
7							
8	345	345	315	225	405	360	315
9							
10	1848	1848	1848	1848	1848	1848	1848
11							
12	5320	5320	5400	5640	5160	5280	5400
13							
14	8835	8835	8775	8595	8955	8865	8775
15							
16	8835	8835	8775	8595	8955	8865	8775
17							
18	5320	5320	5400	5640	5160	5280	5400
19							
20	1848	1848	1848	1848	1848	1848	1848
21							
22	345	345	315	225	405	360	315
23							
24	35	35	45	75	15	30	45
25							
26							
27							
28							
29							
30	1	1	1	1	1	1	1

Table 2.2. $C_1(x)$ and $C_2(x)$ are of odd weight.

$C_1(x)$	1	1	1	1
$C_2(x)$	13556	2767	313151	212050
0	1	1	1	1
2				
4				
6	65	52		51
8	325	390	306	255
10	1430	1313	1972	1717
12	2275	2340	8636	8891
14	2275	2340	20604	21114
16	1430	1313	34017	33507
18	325	390	34017	33507
20	65	52	20604	21114
22			8636	8891
24			1972	1717
26	1	1	306	255
28				51
30				
32				
34			1	1
36				
38				
40				
42				
44				
46				
48				
50				
52				
54				
56				

Table 2.2 (continue). $C_1(x)$ and $C_2(x)$ are of odd weight.

(58, 29, 12) code
C_1 = 1
C_2 = 3172110571

Weight Distribution.

A(0) = A(58) = 1
A(12) = A(46) = 4060
A(14) = A(44) = 35,119
A(16) = A(42) = 306,791
A(18) = A(40) = 1,668,051
A(20) = A(38) = 6,857,949
A(22) = A(36) = 20,988,199
A(24) = A(34) = 47,840,401
A(26) = A(32) = 82,361,972
A(28) = A(30) = 108,372,913

The (58, 29, 12) code with
C_1 = 1
C_2 = 2605667206
has the same weight distribution as above.

Table 2.2 (continue) $C_1(x)$ and $C_2(x)$ are of odd weight.

$C_1(x)$	64272	34175	34175	21654	34175	21654
$C_2(x)$	34175	20361	4274	1405	56300	20361
b	1	1	1	1	1	1
1						
2						
3						
4						
5				3	18	
6	60		15		45	
7	15	120	90	75	45	75
8	150	345	150	210	105	195
9	440		360	395	425	440
10	825		960	933	873	990
11	1860	3360	1800	1755	1605	1620
12	2630	5320	2800	2585	2885	2510
13	3720		3480	3525	3825	3720
14	4590		3990	4425	4335	4470
15	4314	9424	4924	4821	4731	4674
16	4395	8835	4845	4530	4260	4485
17	3720		3480	3705	3435	3720
18	2680		2520	2575	2755	2650
19	1860	3360	1800	1545	1815	1620
20	858	1848	888	915	975	858
21	440		360	500	425	440
22	150		195	195	120	210
23	15	120	90	60	60	75
24	30	35	20	15	30	15
25						
26	15					

Table 2.3 (continue) $C_1(x)$ and $C_2(x)$ are of different weight.

$C_1(x)$	21654	21654
$C_2(x)$	4274	56300
0	1	1
1		
2		
3		
4		
5		18
6	15	30
7	45	60
8	195	135
9	515	360
10	870	948
11	1620	1680
12	2630	2620
13	3600	3900
14	4620	4560
15	4734	4456
16	4245	4275
17	3750	3720
18	2650	2700
19	1620	1680
20	978	900
21	440	450
22	165	210
23	45	60
24	15	5
25	15	
26		

Table 2.3 (continue) $C_1(x)$ and $C_2(x)$ are of different weight.

$C_1(x)$	1405	46517	46517	46517	46517	64272	64272
$C_2(x)$	34175	56300	4274	20361	1405	46517	21654
0	1	1	1	1	1	1	1
1							
2							
3							
4							
5	18	18		15	3	15	
6	30	45		15	30	30	
7	60	60	60	60	75	60	
8	135	90	210	180	120	135	165
9	360	365	500	380	485	300	560
10	948	933	930	930	933	900	1200
11	1680	1665	1560	1680	1545	1860	1200
12	2620	2825	2570	2570	2825	2860	1880
13	3900	3885	3660	3810	3735	3570	4560
14	4560	4275	4530	4560	4245	4080	5520
15	4456	4581	4824	4584	4821	4834	3624
16	4275	4410	4335	4395	4350	4755	3435
17	3720	3495	3660	3660	4395	3420	4560
18	2700	2695	2710	2590	2815	2460	3280
19	1680	1875	1560	1680	1755	1860	1200
20	900	915	918	918	915	948	648
21	450	365	500	455	410	375	560
22	210	180	150	225	105	210	240
23	60	75	60	60	75	75	60
24	5	15	30		45	5	15
25							
26							

Table 2.3 $C_1(x)$ and $C_2(x)$ are of different weight.

2.5 Weight distribution of rate 1/3 and rate 2/3 quasi-cyclic code

A(3m,m) rate 1/3 quasi-cyclic code in systematic form is generated by the circulants $C_1(x)$, $C_2(x)$. Its generator matrix can be expressed as:

$$G = [I, C_1, C_2] \tag{2.17}$$

C_i is a m x m circulant.

Its parity check matrix can be expressed as:

$$H = \begin{bmatrix} C_1^T \\ C2^T \end{bmatrix}, I_{2m} \tag{2.18}$$

Let A_j denote the number of codewords of weight j in the (3m,m) rate 1/3 code and B_i the number of codewords of weight i in the (3m,2m) rate 2/3 code. The McWilliams identities can be expressed (6) in a condensed form as:

$$B_i = 2^{-k} \cdot \sum_{j=0}^{3k} Aj \cdot \sum_{s=0}^{3k} \binom{j}{o} \binom{3k-j}{i-s} (-1)^s \tag{2.19}$$

Each codeword in the (3m,m) rate 1/3 quasi-cyclic code generated by $C_1(x)$ and $C_2(x)$ is of the form:

$$v(x) = [i(x), i(x)C_1(x), i(x)C_2(x)] \bmod (x^m - 1) \tag{2.20}$$

Like in section 2.4, we can have the following remarks for the (3k,k) quasi-cyclic codes in systematic form

i) If $C_1(x)$ and $C_2(x)$ are of odd weight
 - There exists the all one codeword [J,J,J]

ii) If $C_1(x)$ and $C_2(x)$ are of even weight
 - There exists the codeword [J,0,0]

A (3m,2m) rate 2/3 Quasi-Cyclic Code is in the systematic form generated by the circulants $C_1(x)$ and $C_2(x)$. Its generator matrix can be expressed as:

$$G = \left[I_{2m} \; , \; \begin{matrix} C_1 \\ C_2 \end{matrix} \right] \; , \; C_i \text{ is a m x m circulant.}$$

Therefore, its parity check matrix can be expressed as:

$$H = \left[C_1^T, \; C_2^T, \; I_m \right]$$

We can have the following remarks,

i) If $C_1(x)$ and $C_2(x)$ are of odd weight
There exists codewords of the form
$[J,0,J]$, $[0,J,J]$, $[J,J,0]$
All codewords are of even weight

ii) If $C_1(x)$ and $C_2(x)$ are of even weight
There exists codewords of the form
$[J,J,0]$, $[J,0,0]$, $[0,J,0]$
All codewords are of even weight

iii) If $C_1(x)$ is odd and $C_2(x)$ is even
There exists codewords of the form
$[J,J,J]$, $[J,0,J]$, $[0,J,0]$

IV) If $C_1(x)$ is even and $C_2(x)$ is odd
There exists codewords of the form
$[J,J,J]$, $[J,0,0]$, $[0,J,J]$

iii) If $C_1(x)$ is even and $C_2(x)$ is odd
- There exists the codeword $[J,0,J]$
- There are only even weight codewords

IV) If $C_1(x)$ is odd and $C_2(x)$ is even
- There exists the codeword $[J,J,0]$

Generalizing the above discussions to non systematic (3k,k) code, we can summarize:

i) If $C_1(x)$ is odd and $C_2(x)$, $C_3(x)$ are even
- There exists the codeword $[J,0,0]$

ii) If $C_1(x)$,$C_3(x)$ are even and $C_2(x)$ is odd
- There exists the codeword $[0,J,0]$

iii) If $C_1(x)$,$C_2(x)$ are odd and $C_3(x)$ is even
- There exists the codeword $[J,J,0]$

IV) If $C_1(x)$,$C_2(x)$ are even and $C_3(x)$ is odd
- There exists the codeword $[0,0,J]$

V) If $C_1(x)$,$C_3(x)$ are odd and $C_2(x)$ is even
- There exists the codeword $[J,0,J]$
- There are only even codewords

VI) If $C_1(x)$ is even and $C_2(x)$,$C_3(x)$ are odd
- There exists the codeword $[0,J,J]$
- There are only even codewords

VII) If $C_1(x)$,$C_2(x)$ and $C_3(x)$ are odd
- There exists the all-one codeword $[J,J,J]$

Rate (39, 13, 12) code

$C_1(x)$ = 13006 , $C_2(x)$ = 14771

$C_1(x)$ = 14221 , $C_2(x)$ = 13556

$C_1(x)$ = 10550 , $C_2(x)$ = 17227

i	A_i
0,39	1
12,27	156
15,24	858
16,23	1053
19,20	2028

Table 2.4 Weight distribution of quasi-cyclic in systematic form where $C_1(x)$ and $C_2(x)$ are of the same weight.

Rate (39, 13, 11) code

$C_1(x) = 14771$, $C_2(x) = 13556$

$C_1(x) = 17227$, $C_2(x) = 14771$

$C_1(x) = 14221$, $C_2(x) = 13006$

$C_1(x) = 10550$, $C_2(x) = 13556$

$C_1(x) = 10550$, $C_2(x) = 14221$

$C_1(x) = 14221$, $C_2(x) = 14771$

$C_1(x) = 10550$, $C_2(x) = 13006$

$C_1(x) = 17227$, $C_2(x) = 13006$

$C_1(x) = 17227$, $C_2(x) = 13556$

i	A_i
0,39	1
11,28	13
12,27	52
13,26	130
14,25	260
15,24	481
16,23	494
17,22	624
18,21	1066
19,20	975

Table 2.4 (continue)

Rate (39, 13, 9) code

$C_1(x)$ = 14221 , $C_2(x)$ = 17227

$C_1(x)$ = 10550 , $C_2(x)$ = 14771

$C_1(x)$ = 13006 , $C_2(x)$ = 13556

i	A_i
0,39	1
9,30	26
12,27	13
14,25	312
15,24	559
16,23	624
17,22	858
18,21	884
19,20	819

Table 2.4 (continue)

Rate (39, 13, 12) code

$C_1(x) = 7372$, $C_2(x) = 7715$

$C_1(x) = 7372$, $C_2(x) = 5477$

$C_1(x) = 7372$, $C_2(x) = 2767$

$C_1(x) = 7715$, $C_2(x) = 5477$

$C_1(x) = 7715$, $C_2(x) = 2767$

$C_1(x) = 5477$, $C_2(x) = 2767$

i	A_i
0,39	1
12,27	65
13,26	156
14,25	234
15,24	507
16,23	468
17,22	546
18,21	1144
19,20	975

Table 2.4. (continue)

Rate (51, 17, 16) code

$C_1(x) = 264626$; $C_2(x) = 313151$

i	A_i
0,51	1
16,35	1530
19,32	5661
20,31	8160
23,28	24480
24,27	25704

Rate (87, 29, 24) code

$C_1(x) = 3172110571$, $C_2(x) = 2605667206$

i	A_i
0,87	1
24,63	71,253
28,59	613,872
31,56	1,238,793
32,55	5,618,025
35,52	17,276,112
36,51	24,701,040
39,48	62,560,134
40,47	65,315,250
43,44	91,040,976

Table 2.4. (continue)

Rate (39, 13, 9) code.

$C_1(x) = 46517$, $C_2(x) = 34132$, $C_3(x) = 44007$

i	A_i
1,45	1
9,36	5
10,35	3
12,33	15
13,32	45
14,31	150
15,30	345
16,29	615
17,28	1080
18,27	1555
19,26	2310
20,25	3120
21,24	3375
22,23	3765

Table 2.5. Weight distribution of some (39, 13) codes not in systematic form with $C_1(x)$, $C_2(x)$, $C_3(x)$ of odd weight.

Rate (39, 13, 9) code

$C_1(x) = .46517 \cdot$, $C_2(x) = 34175$, $C_3(x) = 44007$

i	A_i
0,45	1
11,34	15
12,33	30
13,32	15
14,31	120
15,30	440
16,29	600
17,28	930
18,27	1715
19,26	2310
20,25	2928
21,24	3560
22,23	3720

Table 2.5. (continue)

$C_1(x)$	64272	64272	64272	64272	64272	64272
$C_2(x)$	34175	21654	34175	21654	21654	21654
$C_3(x)$	20361	56300	1405	20361	34132	44007
A_i						
0	1	1	1	1	1	1
9						
10						
11		15		30		
12	45	15	30		45	45
13	75	90	75	45		
14	180	180	210	150	375	345
15	301	214	289	261		
16	465	450	435	735	1155	1185
17	1080	1275	1095	1080		
18	1655	2075	1685	1545	2950	3115
19	2265	1710	2280	2370		
20	2985	2238	3078	2730	6348	6018
21	3535	4420	3610	3540		
22	3915	4680	3750	4170	7620	7770
23	3855	2940	3570	3480		
24	3545	2600	3380	3300	6780	6870
25	2733	3630	2970	3258		
26	2085	2910	2460	2280	4650	4470
27	1715	1115	1760	1600		
28	1110	795	1020	1110	1935	2145
29	690	810	555	495		
30	293	380	200	288	789	669
31	120	150	165	195		
32	105	45	120	60	120	120
33	15	15	15	30		
34		15	15	15		15

Table 2.6. Weight distribution of some rate 1/3 quasi-cyclic codes where $C_1(x)$, $C_2(x)$, $C_3(x)$ are not of the same weight.

C ( )	64272	64272	46517	46517	64272	64272
C ( )	21654	21654	20361	4272	34175	46517
C ( )	34132	34175	44007	44007	34132	1405
A_i						
0	1	1	1	1	1	1
9						
10						15
11						45
12	45	75	95	35	75	0
13				60		
14	375	285	210	270	270	135
15				154		
16	1155	1110	1275	1425	1170	555
17				1155		
18	2950	3310	3065	3065	3220	1820
19				2310		
20	6348	6078	6168	5808	6168	2838
21				3640		
22	7620	7530	7770	7650	7410	3780
23				3720		
24	6780	6840	6580	7120	6930	3560
25				2790		
26	4650	4620	4680	4680	4710	2205
27				1685		
28	1935	2175	2145	1845	1965	1050
29				660		
30	789	609	644	704	744	365
31				150		
32	120	105	120	150	75	60
33				15		
34		30	15	15	30	

Table 2.6. (continue)

CHAPTER 3

Decoding of binary Quasi-Cyclic Codes

3.1 Introduction

In 1969, Karlin(7)introduced a decoding algorithm which makes Quasi-Cyclic code relatively easy to decode. The algorithm was later extended to rate (m-1)/m code by Shiva and Tavares(8)

There are two main classes of suboptimum soft decision decoding algorithms which are relatively easy to be implemented These are Weldon's algorithm (9) , based on the generalized minimum distance of Forney (10) and the so called Chase's algorithm (11) .

In this chapter, we will show that the structure of Karlin decoder will be more efficient with the channel measurement information.

The following section is devoted to a summary of Karlin's algorithm.

3.2.1 Decoding algorithm for rate 1/2 quasi-cyclic codes.

Let us consider for now the case of rate 1/2 code which can be easily extended to 1/m code.

The transmitted codeword can be written as:

$$v(x) = \left[i(x), i(x)C(x) \right] \mod(x^k-1) \qquad (3.1)$$

Let $e_i(x)$ be the error polynomial in the received information polynomial and $e_p(x)$ be the error polynomial in the received parity polynomial. Then the received codeword can be expressed as:

$$r(x) = \left[i(x)+e_i(x); i(x)C(x)+e_p(x) \right] \qquad (3.2)$$

The presumed parity bits from the received information bits are:

$$\left[(i(x)+e_i(x)).C(x) \right] - \left[i(x).C(x)+e_i(x).C(x) \right] \qquad (3.3)$$

The received parity bits are:

$$\left[(i(x)C(x)+e_p(x)) \right] \qquad (3.4)$$

Let us define the information syndrome

$S_i(x)$ to be (3.3)+(3.4)

$$S_i(x) = i(x)C(x) + e_i(x)C(x) + i(x)C(x) + e_p(x) \quad (3.5)$$

$$= e_i(x)C(x) + e_p(x) \quad (3.6)$$

Let us define the parity syndrome

$$S_p(x) = S_i(x)C^{-1}(x) \quad (3.7)$$

$$= e_i(x) + e_p(x)C^{-1}(x) \quad (3.8)$$

Therefore the two syndromes are

$$S_i(x) = e_i(x)C(x) + e_p(x) \quad (3.9)$$

$$Sp(x) = e_i(x) + e_p(x)C^{-1}(x) \quad (3.10)$$

(3.9) and (3.10) form a system with two unknown $e_i(x)$ and $e_p(x)$.

Since the decoder can correct up to t errors, $t = (d-1)/2$, a received codeword is correctable if and only if

$$W[e_i(x)] + W[e_p(x)] \leq t \quad (3.11)$$

Consider now the case of $e_i(x) = 0$ and $e_p(x) = 0$, then we have from (3.9) and (3.10)

$$S_i(x) = 0 \quad (3.12)$$

$$S_p(x) = 0 \quad (3.13)$$

$$W[S_i(x)] = W[S_p(x)] = 0 \quad (3.14)$$

Now, if errors happen only in the information polynomial then we have also from (3.9) and (3.10)

$$S_i(x) = e_i(x)C(x) \quad (3.15)$$

$$S_p(x) = e_i(x) \quad (3.16)$$

Hence,

$$W\left[S_i(x)\right] > t \tag{3.17}$$

$$W\left[S_p(x)\right] \leq t \tag{3.18}$$

Therefore, the decoding procedure for this case is to evaluate $W\left[S_i(x)\right]$ and $W\left[S_p(x)\right]$, which when equal to (3.17) and (3.18), produce the corrected codeword $V_c(x)$ as:

$$V_c(x) = r(x) + S_p(x) \tag{3.19}$$

Equivalently, if errors happen only in the parity circulant, then we have:

$$S_i(x) = e_p(x) \tag{3.20}$$

$$S_p(x) = e_p(x)C^{-1}(x) \tag{3.21}$$

Hence,

$$W\left[S_i(x)\right] \leq t \tag{3.22}$$

$$W\left[S_p(x)\right] > t \tag{3.23}$$

Therefore, as (3.19), the decoder produces the corrected codeword $V_c(x)$ which is :

$$V_c(x) = r(x) + S_i(x) \tag{3.24}$$

For the case when errors happen in both information and parity polynomial, the decoding is more complex and requires the estimation of $e_i(x)$ and $e_p(x)$

We have:

$$W\left[S_i(x)\right] = W\left[e_i(x)C(x)\right] + W\left[e_p(x)\right] \geq 2t+2 \tag{3.25}$$

$$W\left[S_p(x)\right] = W\left[e_i(x)\right] + W\left[e_p(x)C^{-1}(x)\right] \geq 2t+2 \tag{3.26}$$

The decoding procedure attempts to estimate $e_i(x)$ or $e_p(x)$ such that :

$$\tilde{S_i}(x) = (e_i(x)+\tilde{e_i}(x))C(x) + e_p(x) \tag{3.27}$$

$$\tilde{S_p}(x) = e_i(x) + (e_p(x)+\tilde{e_p}(x))C(x) \tag{3.28}$$

If a good estimation is done i.e.

$$W\left[S_i^{\sim}(x)\right] - W\left[e_p(x)\right] - t \qquad (3.29)$$

$$W\left[S_p^{\sim}(x)\right] - W\left[e_i(x)\right] - t \qquad (3.30)$$

suppose we opt to estimate on $e_i(x)$ and condition (3.29) is met, then :

$$S_i^{\sim}(x) - e_p(x) \qquad (3.31)$$

$$S_p(x) - S_i^{\sim}(x)C^{-1}(x) - e_i(x) \qquad (3.32)$$

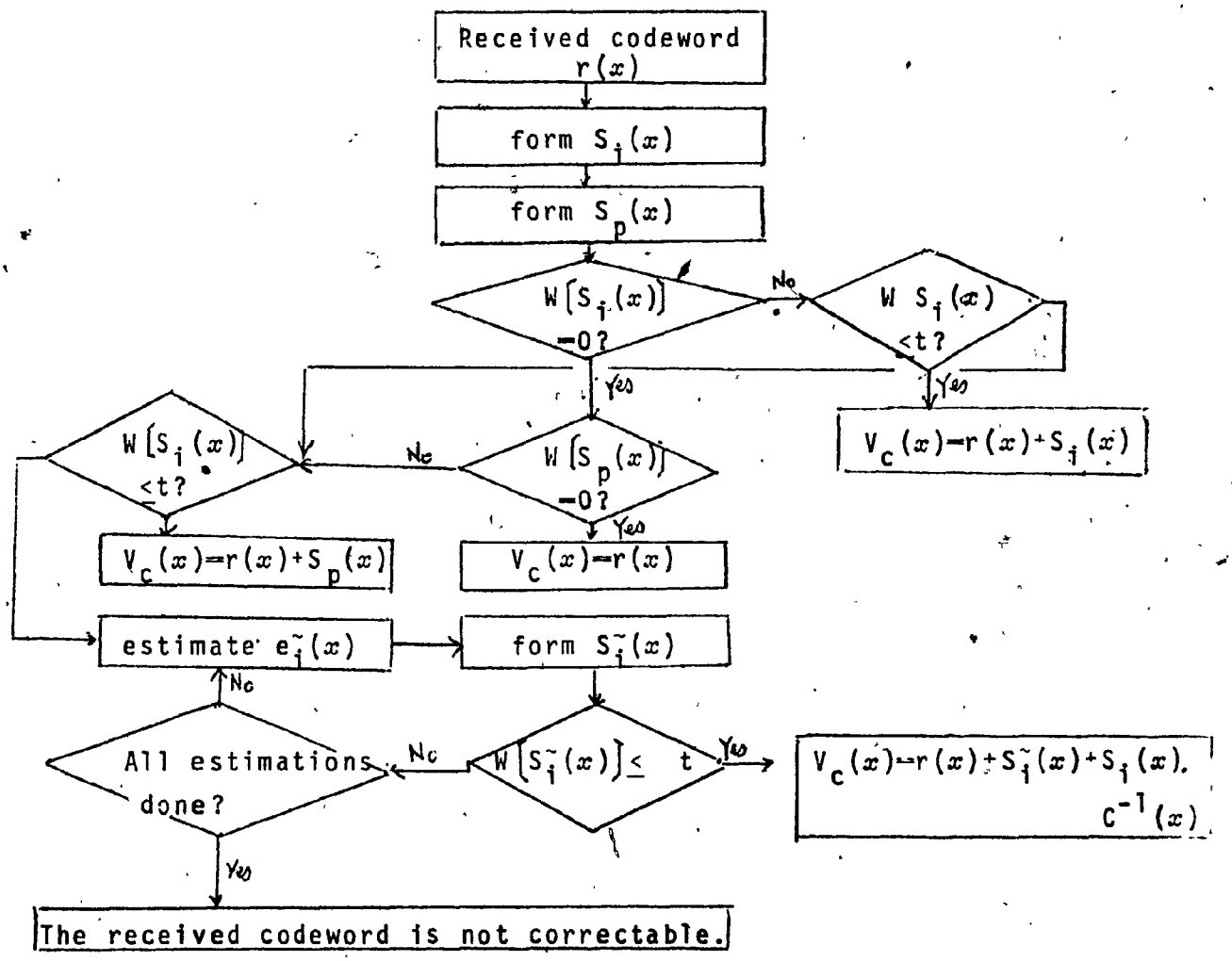
And the corrected codeword will be :

$$V_c(x) - r(x) + S_i^{\sim}(x) + S_i^{\sim}(x)C^{-1}(x) \qquad (3.33)$$

Similarly, if we opt to estimate on $e_p(x)$, the corrected codeword will be

$$V_c(x) - r(x) + S_p^{\sim}(x) + S_p^{\sim}(x)C^{-1}(x) \qquad (3.34)$$

The decoding algorithm therefore can be summarized as in the following flowchart:



3.2.2 Syndrome implemention.

To illustrate the way to implement syndromes, let us consider the code (22,11,6) derived from (23,12,7) perfect Golay code.

The parity circulant $C(x)$ is :

$$C(x) = 1 + x^2 + x^4 + x^7 \quad \text{mod } 2^{11}-1 \tag{3.35}$$

$$C^{-1}(x) = 1 + x^4 + x^7 + x^9 + x^{10} \quad \text{mod } 2^{11}-1 \tag{3.36}$$

The syndromes $S_i(x)$ and $S_p(x)$ can be implemented easily with shift registers with feed back as shown on figure 3.2 and 3.3.

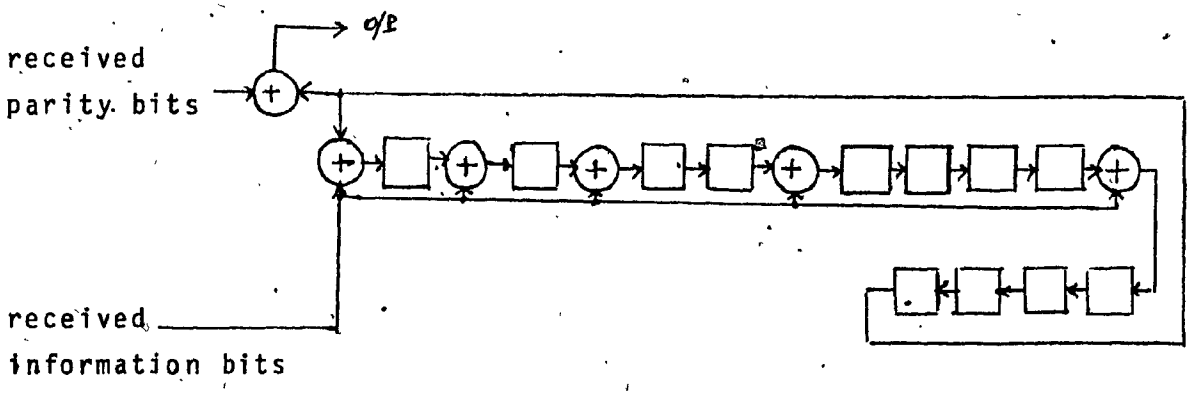


Fig. 3.2 Shift register implemented for calculating $S_i(x) = e_i(x)C(x) + e_p(x)$

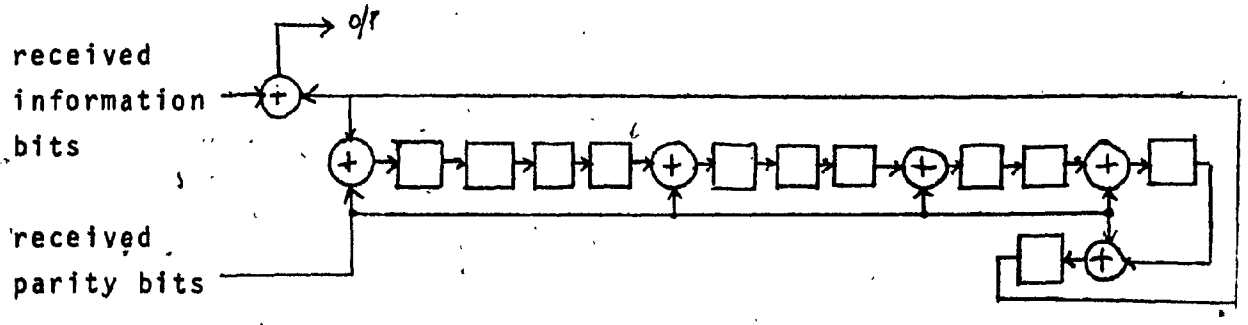


Fig. 3.3 Shift register implemented for calculating $S_p(x) = e_i(x) + e_p(x)C^{-1}(x)$.

3.3 Decoding of rate 2/3 Quasi-Cyclic codes

The principle of decoding rate (m-1)/m is similar to $\frac{1}{m}$ rate since they are based on two kind of syndromes, the information syndrome and the parity syndrome.

Consider now the case of rate 2/3 which can be extended easily to (m-1)/m code.

The transmitted codeword is represented by:

$$V(x) = \left[i_1(x),\ i_2(x),\ i_1(x)C_1(x)+i_2(x)C_2(x)\right] \bmod x^k-1 \qquad (3.37)$$

The received codeword will be :

$$r(x) = \left[i_1(x)+e_i(x),\ i_2(x)+e_{i2}(x),\ i_1(x)C_1(x)+i_2(x)C_2(x)+e_p(x)\right]$$

Similarly to section 3.2, the information syndromes are obtained as :

$$S_{i1}(x) = \left[e_{i1}(x)+e_{i2}(x)C_1^{-1}C_2(x)+e_p(x)C_1^{-1}(x)\right] \qquad (3.38)$$

$$S_{i2}(x) = \left[e_{i2}(x)C_1(x)C_2^{-1}(x)+e_{i2}(x)+e_p(x)C_2^{-1}(x)\right] \qquad (3.39)$$

The parity syndrome can be expressed as :

$$S_p(x) = \left[e_{i1}(x)C_1(x)+e_{i2}(x)C_2(x)+e_p(x)\right] \qquad (3.40)$$

Therefore, the decoding algorithm can be summarize as following :

If no error is made during the transmission,

$$S_{i1}(x) = S_{i2}(x) = S_p(x) = 0 \qquad (3.41)$$

If errors are made only on the information polynomial we have :

$$W\left[S_{i1}(x)\right] \leq t \tag{3.42}$$

$$W\left[S_{i2}(x)\right] > t \tag{3.43}$$

$$W\left[S_{p}(x)\right] > t \tag{3.44}$$

and the corrected codeword $V_c(x)$ will be

$$V_c(x) = r(x) + S_{i1}(x) \tag{3.45}$$

If errors are made only on the information polynomial I_2, we have :

$$W\left[S_{i1}(x)\right] > t \tag{3.46}$$

$$W\left[S_{i2}(x)\right] \leq t \tag{3.47}$$

$$W\left[S_{p}(x)\right] > t \tag{3.48}$$

and the corrected codeword $V_c(x)$ will be

$$V_c(x) = r(x) + S_{i2}(x) \tag{3.49}$$

If errors happen in at least two polynomials, then as explained in section 3.2.1., it requires estimation of $e_{i1}\tilde{}(x)$, $e_{i2}\tilde{}(x)$, $e_{p}\tilde{}(x)$ which when

$$e_{i1}\tilde{}(x) = e_{i1}(x) \tag{3.50}$$

$$e_{i2}\tilde{}(x) = e_{i2}(x) \tag{3.51}$$

$$e_{p}\tilde{}(x) = e_{p}(x) \tag{3.52}$$

give the conditions :

$$W\left[S_{i1}\tilde{}(x)\right] \leq t\text{-}1 \qquad (3.53)$$

$$W\left[S_{i2}\tilde{}(x)\right] \leq t\text{-}1 \qquad (3.54)$$

$$W\left[S_{p}\tilde{}(x)\right] \leq t\text{-}1 \qquad (3.55)$$

therefore, the corrected codeword will be :

$$V_c(x) = r(x)+S_{i1}\tilde{}(x)+S_{i2}\tilde{}(x)+S_{p}\tilde{}(x) \qquad (3.56)$$

3.4 Decoding quasi-cyclic codes with channel measurement information.

As drawn in fig 3.4, our communication system has a pair of encoder / modulator and an another pair of demodulator/ decoder . The natural question then is how to coordinate the design of the modulation system and the coding system so as to produce an efficient and effective communications system.

Suppose that the modulator is M-ary; then, it is understood that "soft decision" means the receiver alphabet is J-ary such that J>M and "hard decision" means J=M.

Usually "soft decision" decoder is understood to be equivalent to a decoder with channel measurement information.

The latter term usually refers to the analog value output of the matched filter.

In this chapter, we want to consider an interactive soft decision algorithm with the Karlin binary decoder. The Karlin binary decoder uses the channel measurement information to optimize its estimating process, when errors happen in more than one polynomial, and the soft decision algorithm discards the guess excluded by the binary decoder, therefore moving into an inner loop.

More than one soft decision algorithm can be used in this interactive process, however we choose the Chase algorithm for two reasons: . It is relatively easy to implement and it can be moved easily into an inner loop.

3.4.1. The Chase algorithm

In 1973, David Chase (11) introduced a significant variation on the theme of decoding binary block code with channel measurement information. The received bits are ordered according to increasing reliability. All the bits which are blanked are not erased and lie on the top of this ordered list. Other unreliable bits are classified according to quantizing errors. Chase suggested that the values of the blanked bits be guessed. For each such guess, a decoding of the entire block is attempted and the decoded error pattern which emerges from ary successes is scored.

The guessing or searching procedure is called "chasing". It is assumed that the algebraic decoding procedure begins afresh for each new guess of the value of the bits in the Chased set. In fact, it is possible to implement chase decoding in a way which moves the chasing into an innermore loop, and thereby attains a modest speed up factor.

In the following, we will summarize the Chase algorithm and explain the process of moving into an "inner loop".

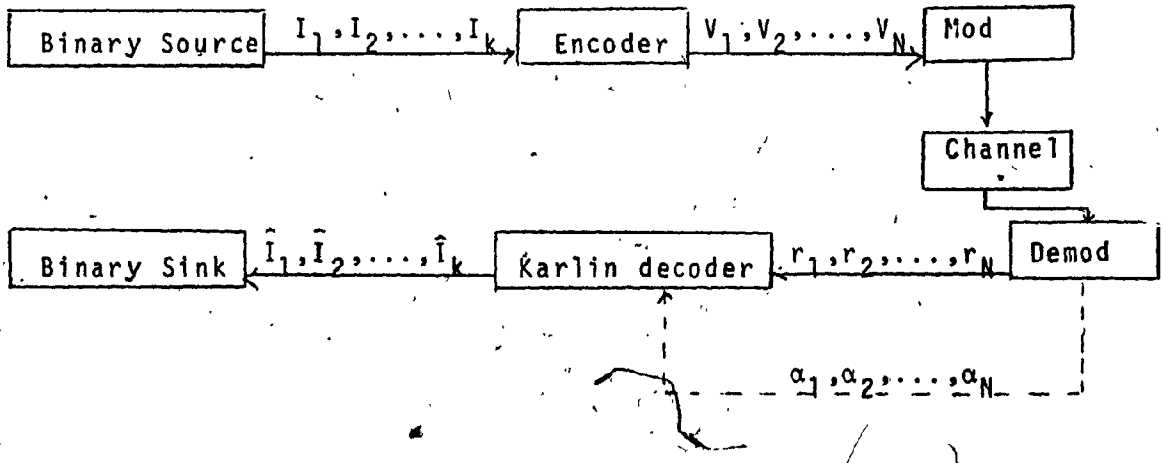


Fig. 3.4 Communication System block diagram.

Let $V_m = V_{m1}, V_{m2}, \ldots, V_{mN}$ be the transmitted codeword. The received codeword is $r = r_1, r_2, \ldots, r_N$. Associated with the received codeword is the channel measurement sequence $\alpha_1, \alpha_2, \ldots, \alpha_N$ which are the analog output of the bank of matched filters.

The error sequence is given by:

$$z_m = r \oplus V_m = r_1 \oplus V_{m1} + r_2 \oplus V_{m2} + \ldots + r_m \oplus V_{mN}, \qquad (3.57)$$

where the notation $\oplus$ represents mod-2 addition.

Let $W(z_m)$ be the binary weight of the sequence z_m as defined in eq.(3.3)

The function of the Karlin binary decoder is to find the codeword, or equivalently the error sequences, that satisfies

$$W(z_m) \leq (d-1)/2 \qquad (3.58)$$

A maximum likelihood decoder (15) can be defined as a decoder such that the decoded codeword satisfies

$$\text{Min} \quad W[r \oplus V_m] \qquad (3.59)$$

where the range of m is over all possible codewords. The difference between this decoder and the hard decision binary decoder is that it can correct more than $(d-1)/2$ in it.

In a similar manner, we can define a complete channel measurement decoder as one that is capable of finding the codeword that satisfies

$$\text{Min}_m \; W_\alpha[r \oplus V_m] \qquad (3.60)$$

In this case we are concerned with finding the error pattern $z_m = r \oplus V_m$ of minimum analog weight, where the analog weight of the sequence z_m is:

$$W_\alpha[z_m] = \sum_{i=1}^{N} \alpha_i z_{mi} \qquad (3.61)$$

The set of error patterns considered is obtained by perturbing the received sequence z with a test pattern T, which is a binary sequence that contains 1's in the location of the digits that are to be inverted. By adding this test pattern, mod 2, to the received sequence, a new sequence

$$z' = z \oplus T \tag{3.62}$$

is obtained. The new error pattern z' obtained by the Karlin binary decoder is added to T, the actual error pattern relative to r is

$$z_T = T \oplus z' \tag{3.63}$$

therefore all error patterns less than (d-1) are correctable.

Chase has also provided three algorithms for estimating T. Amongst those, we are interested in the optimum algorithm #1 and sub-optimum algorithm #2. The mechanism of moving to the inner loop during the decoding process is developed in accordance with the binary Karlin decoder.

Algorithm #1 .

All possible error patterns of binary weight less than or equal to d-1 are considered,

$\binom{N}{d/2}$ test patterns, that are sufficient but not surely necessary are generated.

Needless to say, this algorithm is good for codes whose minimum distance is quite small.

Algorithm #2

Only those error patterns with no more than (d-1)/2 errors located outside the set, which contains the d/2 lowest channel measurements, are considered.

The test patterns T are a combination of 1's which are located in the d/2 positions of lowest confidence by this decoding algorithm.

Let us see now how the decoding process can move into an inner loop.

Let T_1 be the first test pattern. Let us suppose now the Karlin binary decoder has to make p time the error estimations. At the p^{th} error estimation, the error estimated is $\tilde{e}_{1_p}$, the binary decoder decides that $\tilde{e}_{1_p} = e_{1_p}$, or the estimated error pattern is in fact the error pattern.

Instead of throwing out the quantities $\tilde{e}_{1_1}$, $\tilde{e}_{1_1}$,..., $\tilde{e}_{1_{p-1}}$, we form

$$z_{T1_1} = T \oplus \tilde{e}_{1_1} \qquad (3.64)$$

$$z_{T1_2} = T \oplus \tilde{e}_{1_2}$$

...

$$z_{T1_p} = T \oplus \tilde{e}_{1_p}$$

Define R = {T| T is a test pattern defined by algorithm #2}

Subsequently after j estimations, R is reduced to

$$R = \{T \mid T \text{ is a test pattern and } T \text{ is different of } z_{T1_1},\ldots,z_{T1_{p-1}},z_{T2_1},\ldots,z_{T2_{q-1}},\ldots,z_{Tj_1},\ldots,z_{Tj_{s-1}}\} \quad (3.65)$$

This can be seen easily since

$$W_\alpha(z_{T1_p}) < W_\alpha(z_{T1_i}),\ i < p \quad (3.66)$$

$$W_\alpha(z_{T2_q}) < W_\alpha(z_{T2_i}),\ i < q$$

$$W_\alpha(z_{Tj_s}) < W_\alpha(z_{Tj_i}),\ i < s$$

Naturally, R is gradually reduced after each estimation by the Chase algorithm and the search is terminated when R is empty.

Similarly, the Karlin decoder takes into account what estimated error sequences have been already processed before and discard them from its estimation process. This completes and explains the interactive process between the Chase algorithm and the Karlin binary decoder, and also the concept of moving into an inner loop.

3.4.3 The optimal Karlin decoder.

Since its introduction in 1969 by M. Karlin (7) , the structure of the "Karlin decoder" has not been improved

The Karlin decoding process is based on two syndromes, for rate 1/2 code, the parity syndrome and the information syndrome. From eq (3.9) and (3.10),

$$S_i(x) = e_i(x)C(x) + e_p(x)$$

$$S_p(x) = e_i(x) + e_p(x)C^{-1}(x)$$

This is a system of 2 equations and in general, $e_i(x)$ and $e_p(x)$ should be estimated. Therefore for long code, the estimation process is lengthy and the decoder seems to be locked into an infinite time of processing.

As an example consider a rate 1/2, (26,13,7) quasi-cyclic code. If errors happen in both information and parity polynomials, at least one estimation should be produced and at most

$$\binom{13}{1} + \binom{13}{2} = 91 \text{ estimations}$$

No successful efforts are known how to optimize or rationalize the estimation process from the algebraic structure of quasi-cyclic codes point of view.

However looking to associate each received bit with a value of channel measurement α_i , the estimation process can be sped up.

Associated with each bit is the analog value α_i output of the matched filter. The most reliable bit has its $\alpha_i = 1$ and the erased bit has its $\alpha_i = 0$

Therefore, the estimating sequence $\tilde{e_i}(x)$ or $\tilde{e_p}(x)$ will be done sequentially. For example, let us consider the first estimated errors sequence $\tilde{e_i}(x)$

$$\tilde{e_{i1}}(x) = x^k + x^l + \ldots + x^m \tag{3.67}$$

such that

$$\tilde{\alpha_{ei1}}(x) = \alpha_x{}^k + \alpha_x{}^l + \ldots \quad \alpha_x{}^m \tag{3.68}$$

has the smallest value .

Therefore

$$\tilde{\alpha_{ei1}}(x) \leq \tilde{\alpha_{ei2}}(x) \leq \tilde{\alpha_{ei3}}(x) \ \ldots \leq \tilde{\alpha_{eis}}(x) \tag{3.69}$$

Naturally $\tilde{e}_{is}(x) = e_i(x)$

This completes our discussion about the optimal way to estimate the error sequence with channel measurement information.

CHAPTER 4

POWER RESIDUES CODES AND THE GENERATION OF QUASI-CYCLIC CODE BY THE NORMAL BASIS THEOREM.

4.1 Introduction : Power residue codes are very good codes, however, they are hard to decode (2) one advantage in expressing power residue codes in Quasi-Cyclic is that they can be decoded easily by the Karlin decoder. In this chapter, we will review the automorphism group of $GF(p^m)$, the theorem of Normal basis, the definition of the s^{th} power residue code. Based on the Normal basis theorem, the Quasi-Cyclic codes are generated from power residue codes. Also, their sub-codes are generated and a figure of comparison between some good sub-codes and the best codes from appendix A & 1 of McWilliams & Sloane (12) is shown on Table 5.2.

4.2 The automorphism group of $GF(p^m)$

Associated with the field $GF(p^m)$ is the set of mappings, called automorphisms, of the field onto itself and leaving the ground field GF(p) fixed, such a mapping is denoted:

$$\sigma:\beta\rightarrow\beta^{\sigma}$$

We have the following definition

Definition: An automorphism of $GF(p^m)$ over GF(p) is a mapping which fixes the elements of GF(p) and has the properties

i) $(\alpha+\beta)^{\sigma} = \alpha^{\sigma} + \beta^{\sigma}$

ii) $(\alpha\beta)^{\sigma} = \alpha^{\sigma}\cdot\beta^{\sigma}$

iii) $\alpha^{\sigma\cdot\tau} = (\alpha^{\sigma})^{\tau}$ where $\sigma\cdot\tau$ is the product of σ and τ.

This group is called the automorphism group of Galois group of $GF(p^m)$.

Example : $GF(2^3) = \{0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6\}$ with $\alpha^6 = \alpha^2+1$

$\alpha^7 = 1$

Let us consider the mapping identity 1, it leaves all elements fixed.

Let us consider the mapping $\sigma = 2$

$0^2 \to 0$

$1^2 \to 1$

$\alpha^2 \to \alpha^2$

$(\alpha^2)^2 \to \alpha^4$

$(\alpha^3)^2 \to \alpha^6$

$(\alpha^4)^2 \to \alpha$

$(\alpha^5)^2 \to \alpha^3$

$(\alpha^6)^2 \to \alpha^5$

We observe that the elements of the ground field are fixed and other elements of $GF(2^3)$ are permuted.

It is known that the automorphism group of $GF(p^m)$ is a cyclic group of order m consisting of the mapping:

$\sigma p : \beta \to \beta^r$ and its power

Thus for $GF(p^m)$, $\sigma p = \{1,p,p^2,\ldots,p^{m-1}\}$

For above example, $GF(2^3)$, $\sigma_2 = \{1,2,4\}$

4.3 The Normal bases

It is known that $GF(p^m)$ is a vector space of dimension m over GF(p). Any set of m linearly indepent elements can be used as a basis for this vector space.

In constructing $GF(p^m)$ from a primitive irreducible polynomial $p(x)$, we use the basis $\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \ldots, \alpha^{2^{(m-1)}}$, where α is a zero of $p(x)$.

We will accept the following without proofs. For proofs, see (12)

Definition 4.3.1 A normal base of $GF(p^m)$ over GF(p) is a base of the form $\{\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \ldots, \alpha^{2^{(m-1)}}\}$ where α is a primitive element.

For example: The normal base of $GF(2^3)$ is $\{\alpha, \alpha^2, \alpha^4\}$

Theorem 4.3.2 For a $GF(p^m)$, the normal base is unique.

Since all finite fields of order p^m are isomorphic, it follows there is a one to one mapping from one field to another one. Since the class of mapping σp is a power of p, the base $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{(m-1)}}\}$ is unique.

Since there always exists an irreducible polynomial of degree m, $m > 0$, we have the following theorem:

Theorem 4.3.3 A Normal basis exists in any field $GF(p^m)$

The following Corollary, is a refinement of theorem 5.3.3, due to Davenport (12).

Corollary 4.3.4 Any finite field $GF(p^m)$ contains a primitive element α such that $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{(m-1)}}\}$ is a normal basis.

If the generating polynomial is irreducible and has roots independant, then for the field $GF(p^m)$, the normal basis is given by $\{\alpha, \alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{m-1}}\}$ and any element β of $GF(p^m)$ can be expressed as a unique expression of the form:

$$\beta = a_0\alpha + a_1\alpha^p + a_2\alpha^{p^2} + \ldots + a_{m-1}\alpha^{p^{m-1}} \qquad (4.1)$$

Let us consider the power of

$$\beta^p = a_0\alpha^p + a_1\alpha^{p^2} + a_2\alpha^{p^3} + \ldots + a_{m-1}\alpha^{p^m} \qquad (4.2)$$

$$= a_{m-1}\alpha + a_0\alpha^p + a_1\alpha^{p^2} + \ldots + a_{m-2}\alpha^{p^{m-1}} \qquad (4.3)$$

$$\vdots$$

$$\beta^{p^{m-1}} = a_1\alpha + a_2\alpha^p + a_3\alpha^{p^2} + \ldots + a_0\alpha^{p^{m-1}}$$

Expressing $\beta, \beta^p, \ldots, \beta^{p^{m-1}}$ in the matrix form where β is a column vector:

$$\{\beta, \beta^p, \ldots, \beta^{p^{m-1}}\} = \begin{bmatrix} a_0 & a_{m-1} & \cdots & a_1 \\ a_1 & a_0 & & a_2 \\ \vdots & \vdots & & \vdots \\ a_{m-1} & a_{m-2} & \cdots & a_0 \end{bmatrix} \quad m \times m \qquad (4.4)$$

Thus, the field elements $\beta, \beta^p, \ldots, \beta^{p^{m-1}}$ represent a circulant matrix of dimension m x m.

4.4 The s^{th} power residue

The concept of power residue is a generalization of the Quadratic Reciprocity Law of Gauss. The basis concept of Quadratic Congruences is given in chapter 1, $x^2 \equiv n \pmod p$ for an odd prime p with $(p,n) = 1$. A natural extension is to replace 2 by m, thus having the m^{th} order congruence $x^m \equiv n \pmod p$.

We can state the following definition of power residue (1).

4.4.1 Definition If $x^m \equiv n \pmod p$ is solvable with p an odd prime, $(p,n) = 1$ and $m \geq 1$, then n is called an m^{th} power residue moduls p.

Let q be a primitive root mod p, then $x^m \equiv n \pmod p$ is solvable if $n \equiv q^{kd} \pmod p$ where k is an integer and $d \equiv (p-1,m)$

Then we have the following theorem:

Theorem 4.4.2 Let p be an odd prime with $(p,n) = 1$, let m be a positive integer, and let $d = (p-1,m)$. Then $x^m \equiv n \pmod p$ is solvable when $n^{(p-1)/d} \equiv 1 \pmod p$

Proof: Suppose $n^{(p-1)/d} = 1 \pmod p$. Then $(n,p) \equiv 1$. There exists some integer t such that $n = q^t \pmod p$ where q is a primitive root modulo p.

Therefore,

$$q^{t(p-1)/d} \equiv n^{(p-1)/d} \equiv 1 \pmod p \qquad (4.6)$$

Since q is primitive root mod p, q belongs to (p-1) mod p or:

$$(p-1) \mid (p-1) \cdot \frac{t}{d} \qquad (4.7)$$

This implies $t/d = k$ integer

Then:

$n \equiv q^{kd} \pmod p$ and $x^m \equiv n \pmod p$ is solvable

It follows also from generalization of Quadratic Residues that there are $(p-1)/d$ with power residues mod p, p odd prime where $d = (p-1,m)$

Theorem 4.4.3 Let p be an odd prime, let q be a primitive root mod p, and let $d = (m,p-1)$ where $m \geq 1$. Then the m^{th} power residues mod p are $q^d, q^{2d}, \ldots, q^{d(p-1)/d}$.

As stated, all q^{kd} are m^{th} power residues. They are mutually incongruent mod p and there are in all $(p-1)/d$ m^{th} power residues.

4.5 Power Residue Codes

Let m be the multiplicative order of p mod n. Suppose that m divides $(n-1)/s$ i.e.

$$n = ems + 1 \qquad (4.8)$$

e integer

Then we have following definition:

Definition 4.5.1 An s-th power residue code of length n is defined as a cyclic code over GF(p) with a check polynomial of the form:

$$h(x) = \prod_{r \in R} (x - \beta^r) \qquad (4.9)$$

where R is the set of incongruent s-th power residue mod n and β is a primitive n-th root of 1 over GF(p)

As a result of the definition, there are several facts of importance that can be mentioned (12)

1) There are em elements in R, as shown by theorem 5.4.3

2) The number of information digits is equal to em. The degree of $h(x)$, equal to the number of information digits, is equal to m.

3) Since x^n-1 always factors into irreducible polynomials whose degree divides (n-1) :

$$x^n - 1 = (x+1)T_p(x) \qquad (4.10)$$

Let n be a prime of the form $8\mu \pm 1$, for which 2 is a primitive nonresidue of n. Then $T_p(x)$ will be irreducible.

Let n be a prime of the form $8a\pm1$, for which 2 is a quadratic residue of n, then $T_p(x)$ can be factorized into two reprocical irreducible polynomials

Since $n = ems+1$, then x^n-1 can be factorized into (es+1) irreducible polynomials whose degree divides (n-1)

$$x^n-1 = (x+1)f_1(x)f_2(x)\ldots f_{es}(x) \qquad (4.11)$$

Let α_i be the root of $f_i(x)$, m_i be the degree of $f_i(x)$

$$(\beta_i)^{p^{mi}} = \beta_i \quad \text{(Fermat Theorem)} \qquad (4.12)$$

Since n is prime, $p^{mi} \equiv 1 \pmod n$. Or $p^m \equiv 1 \pmod n$, mi is equal to m:

Hence the es irreducible polynomials $f_1(x),\ldots,f_{es}(x)$ all have degree m.

4) The set R forms a multiplicative group of order em. The index of R in GF(p) is s.

5) The generator matrix of an s^{th} power residue code can be put into the form:

$$G = \begin{bmatrix} 1 & \beta & \ldots & \beta^{n-1} \\ 1 & \beta^{j-1} & \ldots & \beta^{j1(n-1)} \\ \vdots & \vdots & & \\ 1 & (\beta^{(je-1)}) & & \beta^{(je-1)(n-1)} \end{bmatrix} \qquad (4.13)$$

for the case e = 1

$$G = \begin{bmatrix} 1 & \beta & \ldots & \beta^{n-1} \end{bmatrix} \qquad (4.14)$$

Let G' be:

$$G' = \begin{bmatrix} \beta & \beta^2 & \ldots & \beta^{n-1} \end{bmatrix} \qquad (4.15)$$

Regrouping all the roots of the seme set of incongruent

$$G' = \begin{bmatrix} (\beta\ \beta^2\ \beta^4\ \ldots)\ (\beta^3\ \beta^6\ \ldots)\ (\beta^5\ \beta^{10}\ \ldots) \end{bmatrix} \qquad (4.16)$$

As demonstrated in section 5.3, $[\beta,\beta^2,(\beta^p)^{m-1}]$ can be expressed as a m x m circulant matrix.

Thus:

$G' = [C_1 \quad C_2 \ldots C_m]$, C_i is a m x m circulant matrix

If any C_i is invertible, then

$G' = [I \quad C_1 \ldots C_{m-1}]$

Therefore, we have the following theorem due to Chen (5)

Theorem 4.5.2 The s^{th} power residue codes with the first digit deleted are equivalent to quasi-cyclic codes.

Consider the case p=2, m=3, C=1, s=7. We know there exists a (7,3) Hamming Code with minimum distance $d_{min}=4$.

Let $\alpha, \alpha^2, \alpha^4$ form the normal basis. The primitive 7^{th} root of unity is $\beta = \alpha^{(2^3-1)/7} = \alpha$. Expressing β, β^3 under the normal basis of $\{\alpha, \alpha^2, \alpha^4\}$, we can have G' as:

$G' = [C_1 \quad C_2]$

One special case of interest is for p=2 and $n=2^m-1$. Then, the s^{th} power residue code is reduced to maximum length sequence code. Then, the maximum length sequence codes with one digit delected are equivalent to quasi-cyclic codes. This class of codes is majority logic decodable.

Ex:

$2^3-1 = 7$, the QC code is (6,3)

$2^5-1 = 31$, the QC code is (30,5)

$2^7-1 = 127$, the QC code is (126,7)

4.6 Some weight distribution of Quasi-Cyclic codes derived from power residue codes.

A computer program is written to generate the Normal Basis, and compute the set of elements $\alpha, \alpha^p, \ldots, \alpha^{pm-1}$ Some Quasi-Cyclic codes are developed and their weight distribution computed.

Table 4.1 : Quasi-Cyclic Codes derived form power residue codes.

(30,5,15) Quasi-Cyclic code

$C_1 = 1$, $C_2 = 11$ $C_3 = 30$, $C_4 = 35$, $C_5 = 26$, $C_6 = 31$.

The weight distribution is :

A(0) = 1

A(15) = 16

A(16) = 15

(72,9,27) Quasi-Cyclic code.

$C_1 = 233$, $C_2 = 310$, $C_3 = 557$, $C_4 = 454$, $C_5 = 372$,
$C_6 = 624$, $C_7 = 572$, $C_8 = 560$.

The weight distribution is :

A(0) = 1

A(27) = 28

A(28) = 45

A(35) = 108

A(36) = 111

A(39) = 120

A(40) = 99

(88,11,39) Quasi-Cyclic code.

$C_1 = 1253$, $C_2 = 1467$, $C_3 = 2224$, $C_4 = 1355$, $C_5 = 1541$,
$C_6 = 2547$, $C_7 = 2621$, $C_8 = 3145$

The weight distribution is :

A(0) = 1
A(39) = 440
A(40) = 539
A(47) = 528
A(48) = 451
A(55) = 56
A(56) = 33

(150,15,59) Quasi-Cyclic code.

$C_1 = 1405$, $C_2 = 34175$, $C_3 = 64272$, $C_4 = 21654$,
$C_5 = 46517$, $C_6 = 56300$, $C_7 = 4274$, $C_8 = 20361$,
$C_9 = 34132$, $C_{10} = 44007$.

The weight distribution is :

A(0) = 1
A(59) = 180
A(60) = 273
A(63) = 320
A(64) = 435
A(67) = 2040
A(68) = 2490
A(71) = 4680
A(72) = 5135
A(75) = 2964
A(76) = 2925
A(79) = 2400

A(80) = 2130

A(83) = 3360

A(84) = 2680

A(87) = 440

A(88) = 315

4.7 Sub-Codes of Quasi-Cyclic Codes

If a Quasi-Cyclic code can be defined by its generator matrix G as:

$$G = [C_1, C_2, \ldots, C_s] \tag{4.17}$$

where C_i is a m x m circulant matrix, a sub-code is also defined by its generator matrix G' such that

$$G' = [C_1, C_2, \ldots, C_r] \tag{4.18}$$

with $s > r \geq 2$

Low rate code such as rate $\frac{1}{10}$, $\frac{1}{8}$ quasi-cyclic codes have numerous sub-codes.

For rate $\frac{1}{10}$, (150,15) quasi-cyclic code, there are in all

$\binom{10}{1}$ (135,15) rate $\frac{1}{9}$ sub-codes.

$\binom{10}{2}$ (120,15) rate $\frac{1}{8}$ sub-codes.

$\binom{10}{3}$ (105,15) rate $\frac{1}{7}$ sub-codes.

$\binom{10}{4}$ (90,15) rate $\frac{1}{6}$ sub-codes.

$\binom{10}{5}$ (75,15) rate $\frac{1}{5}$ sub-codes.

$\binom{10}{6}$ (60,15) rate $\frac{1}{4}$ sub-codes.

$\binom{10}{7}$ (45,15) rate $\frac{1}{3}$ sub-codes.

$\binom{10}{8}$ (30,15) rate $\frac{1}{2}$ sub-codes.

and for the (88,11) quasi-cyclic code

$\binom{8}{1}$ (77,11) rate $\frac{1}{7}$ sub-codes.

$\binom{8}{2}$ (66,11) rate $\frac{1}{6}$ sub-codes.

$\binom{8}{3}$ (55,11) rate $\frac{1}{5}$ sub-codes.

$\binom{8}{4}$ (44,11) rate $\frac{1}{4}$ sub-codes.

$\binom{8}{5}$ (33,11) rate $\frac{1}{3}$ sub-codes.

$\binom{8}{6}$ (22,11) rate $\frac{1}{2}$ sub-codes.

They are so numerous and quite good. The best can be as good or better than those listed in McWilliams & Sloane (12).

We note that McWilliams & Sloane (12) give only the list of best codes of minimum distance less than 29.

Table 5.2 gives some good sub-codes and compares them with those listed in McWilliams & Sloane.

It is a substantial task to list all these sub-codes, in section 5.7.2 and 5.7.3 we give the weight distribution of some very good sub-codes which we are able to list.

n	k	Best d_{min} of Subcode	Minimum distance of best known codes Mc Williams & Sloane	
55	11	20		
55	11.585		21	Nonlinear Code, construction Y2
66	11	26		
66	12		27	Delsarte-Goethals generalized Kerdock code (nonlinear)
77	11	32		
77	14.248		29	Zinoviev's construction of concatenated codes
90	15	31		
90	19		29	Zinoviev's construction of concatenated codes
105	15	37		
88	11	39		
120	15	44		
135	15	50		
150	15	59		

Table 5.2 Figure of comparison between some good sub-codes and the best codes from appendix A&1 of Mc Williams & Sloane (12)

5.7.2. Sub-Codes derived from (150, 15) Quasi-Cyclic Code.

(135, 15, 48) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 1405$, $C_3(x) = 34175$,
$C_4(x) = 64272$, $C_5(x) = 21654$, $C_6(x) = 56300$,
$C_5(x) = 4274$, $C_6(x) = 20361$, $C_7(x) = 34132$.

i	A_i
0	1
48	15
50	33
52	60
54	345
56	450
58	840
60	2256
62	3514
64	4665
66	4510
68	3480
70	2733
72	2870
74	3900
75	2460
78	1180
80	255
82	105

(135, 15, 50) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 1405$, $C_3(x) = 34175$,
$C_4(x) = 64272$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$, $C_9(x) = 34132$.

i	A_i
0	1
50	33
52	135
54	290
56	405
58	885
60	2256
62	3510
64	4635
66	4575
68	3345
70	2928
72	2735
74	2985
76	2640
78	960
80	360
82	90

(135, 15, 49) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 4274$,
$C_7(x) = 20361$, $C_8(x) = 34132$, $C_9(x) = 44007$.

i	A_i	i	A_i
0	1	67	1320
49	15	68	1425
50	15	69	1920
52	45	70	1755
53	150	71	975
54	225	72	990
55	105	73	2175
56	120	74	1605
57	395	75	1204
58	495	76	900
59	660	77	945
60	878	78	835
61	1785	79	225
62	2145	80	135
63	1655	81	95
64	1650	82	60
65	2760		
66	3105		

(135, 15, 49) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 20361$, $C_8(x) = 34132$, $C_9(x) = 44007$.

i	A_i	i	A_i
0	1	67	1740
49	15	68	1875
50	3	69	1475
51	30	70	1350
52	75	71	1395
53	60	72	1415
54	195	73	1635
55	210	74	1290
56	120	75	1641
57	290	76	1095
58	525	77	855
59	810	78	680
60	1080	79	240
61	1470	80	210
62	1515	81	45
63	2175	82	30
64	2370	83	15
65	2283	84	15
66	2540		

(135, 15, 47) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 34132$, $C_9(x) = 44007$.

i	A_i	i	A_i
0	1	66	2450
47	15	67	1920
50	18	68	1710
51	15	69	1550
52	15	70	1320
53	105	71	1320
54	195	72	1520
55	195	73	1620
56	255	74	1380
57	275	75	1536
58	375	76	1110
59	765	77	840
60	1065	78	605
61	1485	79	315
62	1740	80	225
63	2175	81	60
64	2355	82	45
65	2193		

(135, 15, 50) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$, $C_9(x) = 44007$.

i	A_i
0	1
50	15
52	165
54	285
56	420
58	855
60	2277
62	3450
64	4740
66	4435
68	3360
70	3195
72	2420
74	3195
76	2415
78	1150
80	315
82	60
84	15

(135, 15, 50) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$, $C_9(x) = 34132$.

i	A_i
0	1
50	30
52	105
54	390
56	240
58	1260
60	1617
62	4260
64	3645
66	5680
68	2595
70	3510
72	1940
74	3900
76	1875
78	1360
80	270
82	90

(135, 15, 49) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 12654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$, $C_9(x) = 34132$.

i	A_i	i	A_i
0	1	67	1950
49	15	68	1665
51	30	69	1580
52	75	70	1500
53	90	71	1365
54	180	72	1280
55	165	73	1515
56	180	74	1590
57	395	75	1464
58	450	76	1110
59	660	77	1035
60	918	78	545
61	1455	79	210
62	1815	80	195
63	2220	81	75
64	2640	82	75
65	2160		
66	2165		

(135, 15, 50) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 1405$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$, $C_9(x) = 34132$.

i	A_i
0	1.
50	33
52	120
54	290
56	450
58	945
60	2107
62	3540
64	4695
66	4435
68	3525
70	2868
72	2780
74	3045
76	2385
78	1070
80	450
82	30
84	5

(135, 15, 49) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 1405$, $C_3(x) = 34175$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$, $C_9(x) = 34132$.

i	A_i	i	A_i
0	1	67	1785
49	15	68	1755
50	3	69	1565
51	50	70	1545
52	60	71	1515
53	60	72	1220
54	180	73	1305
55	180	74	1260
56	195	75	1816
57	330	76	1380
58	435	77	810
59	675	78	575
60	1065	79	225
61	1665	80	165
62	1680	81	50
63	1980	82	60
64	2415	83	30
65	2328		
66	2390		

(120, 15, 40) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 20361$, $C_3(x) = 1405$,
$C_4(x) = 64272$, $C_5(x) = 21654$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i	i	A_i
0	1	59	2340
40	3	60	2165
41	15	61	1665
44	15	62	1710
45	61	63	1830
46	60	64	1575
47	90	65	1788
48	210	66	1480
49	270	67	1200
50	390	68	960
51	680	69	870
52	780	70	720
53	1020	71	270
54	1470	72	165
55	1890	73	120
56	2190	74	60
57	2255	75	20
58	2430		

(120, 15, 42) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 20361$, $C_3(x) = 34175$,
$C_4(x) = 64272$, $C_5(x) = 21654$, $C_6(x) = 21654$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i
0	1
42	30
44	15
46	150
48	420
50	768
52	1515
54	3005
56	4470
58	4680
60	4121
62	3360
64	3555
66	3000
68	1965
70	1173
72	450
74	90

(120, 15, 40) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 1405$, $C_3(x) = 34175$,
$C_4(x) = 64272$, $C_5(x) = 21654$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i
0	1
40	3
42	15
44	60
46	105
48	405
50	780
52	1560
54	3050
56	4215
58	4905
60	4124
62	3525
64	3150
66	3090
68	2160
70	1080
72	450
74	90

(120, 15, 42) Sub-Code

$C_1(x)$ — 20361 , $C_2(x)$ — 1405 , $C_3(x)$ — 34175 ,
$C_4(x)$ — 21654 , $C_5(x)$ — 46517 , $C_6(x)$ — 45300 ,
$C_7(x)$ — 4274 , $C_8(x)$ — 44007 .

i	A_i
0	1
42	15
44	60
46	165
48	245
50	831
52	1694
54	3135
56	4155
58	4575
60	4141
62	3795
64	3090
66	3225
68	2025
70	1065
72	445
74	90
76	15

(120, 15, 40) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 34132$.

i	A_i
0	1
40	15
44	45
46	150
48	405
50	595
52	1500
54	3110
56	4650
58	4365
60	4286
62	3600
64	2970
66	3120
68	2250
70	1140
72	375
74	75
76	15

(120, 15, 42) Sub-Code

$C_1(x) = 20361$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i
0	1
42	15
44	60
46	135
48	390
50	750
52	1455
54	3245
56	4320
58	4680
60	4022
62	3675
64	3195
66	3060
68	2145
70	1065
72	510
74	15
76	30

(120, 15, 40) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i
0	1
40	15
44	30
46	120
48	420
50	846
52	1530
54	2075
56	4425
58	4530
60	4286
62	3585
64	3165
66	3090
68	2130
70	1065
72	510
74	30
78	15

(120, 15, 42) Sub-Code

$C_1(x) = 20361$, $C_2(x) = 1405$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i	i	A_i
0	1	61	1815
42	15	62	1845
43	15	63	1785
44	15	64	1470
45	46	65	1710
46	60	66	1390
47	150	67	1390
48	240	68	1065
50	273	69	825
51	560	70	600
52	810	71	270
53	1230	72	255
54	1515	73	75
55	1863	74	45
56	2190	75	35
57	2330		
58	2385		
59	2055		
60	2210		

(120, 15, 44) Sub-Code

$C_1(x)$ - 20361 , $C_2(x)$ - 1405 , $C_3(x)$ - 34175 ,
$C_4(x)$ - 64272 , $C_5(x)$ - 46517 , $C_6(x)$ - 56300 ,
$C_7(x)$ - 4274 , $C_8(x)$ - 44007 .

i	A_i	i	A_i
0	1	61	1894
44	30	62	1890
45	106	63	1790
46	105	64	1395
47	105	65	1680
48	165	66	1310
49	135	67	1230
50	393	68	1215
51	605	69	950
52	660	70	585
53	1305	71	300
54	1520	72	170
55	2073	73	90
56	2265	74	45
57	1995	76	30
58	2280		
59	2025		
60	2295		

(120, 15, 43) Sub-Code

$C_1(x) = 20361$, $C_2(x) = 1405$, $C_3(x) = 34175$,
$C_4(x) = 64272$, $C_5(x) = 21654$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 44007$.

i	A_i	i	A_i
0	1	61	1830
43	30	62	1740
44	15	63	1770
45	46	64	1410
46	90	65	1620
47	90	66	1395
48	255	67	1455
49	270	68	1185
50	273	69	770
51	615	70	645
52	675	71	270
53	1170	72	140
54	1725	73	105
55	1878	74	75
56	2010	75	30
57	2125		
58	2505		
59	2310		
60	2245		

(120, 15, 43) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 4274$, $C_8(x) = 20361$.

i	A_i	i	A_i
0	1	61	1935
43	15	62	1485
44	45	63	1650
45	49	64	1590
46	30	65	1620
47	120	66	1440
58	255	67	1395
49	300	68	1200
50	330	69	905
51	615	70	540
52	690	71	225
53	1095	72	230
54	1530	73	120
55	1605	74	15
56	2340	75	15
57	2680	78	15
58	2295		
59	2040		
60	2353		

(105, 15, 37) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 1405$,
$C_7(x) = 44007$.

i	A_i	i	A_i
0	1	55	2310
37	30	56	1845
38	60	57	1725
39	60	58	1290
40	93	59	1365
41	225	60	1175
42	320	61	780
43	375	61	465
44	496	63	290
45	786	64	255
46	1245	65	93
47	1740	66	65
48	1950	67	30
49	2445		
50	2565		
51	2150		
52	2250		
53	1980		
54	2310		

(105, 15, 36) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 46517$,
$C_7(x) = 44007$.

i	A_i
0	1
36	15
38	90
40	255
42	550
44	1080
46	2460
48	3990
50	4938
52	4875
54	3905
56	3735
58	3210
60	2126
62	990
64	435
66	110
70	3

(105, 15, 36) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 1405$, $C_6(x) = 46517$,
$C_7(x) = 44007$.

i	A_i	i	A_i
0	1	54	2100
36	15	55	2220
37	15	56	1590
38	30	57	1860
39	50	58	1590
40	138	59	1140
41	270	60	1055
42	230	61	810
43	390	62	630
44	615	63	345
45	826	64	120
46	1080	65	93
47	1785	66	95
48	2055	67	15
49	2025	69	5
50	2565		
51	2375		
52	2475		
53	2160		

(105, 15, 36) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 34132$.

i	A_i
0	1
36	30
38	60
40	291
42	450
44	1215
46	2370
48	4160
50	4755
52	4590
54	4670
56	3285
58	3030
60	2301
62	1140
64	255
66	165

(105, 15, 36) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 21654$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 44007$.

i	A_i
0	1
36	60
38	15
40	231
42	570
44	1080
46	2625
48	4025
50	4725
52	4560
54	4475
56	3615
58	3030
60	2166
62	1125
64	360
66	75
68	30

(105, 15, 36) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 34175$, $C_3(x) = 64272$,
$C_4(x) = 4274$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 44007$.

i	A_i
0	1
36	15
38	60
40	243
42	650
44	1050
46	2550
48	3905
50	4860
52	4575
54	4375
56	3705
58	3030
60	2304
62	960
64	330
66	140
70	15

(105, 15, 36) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 34175$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 46517$, $C_6(x) = 56300$,
$C_7(x) = 44007$.

i	A_i
0	1
36	35
38	75
40	228
42	405
44	1470
46	2190
48	4085
50	4875
52	4800
54	3975
56	3990
58	2715
60	2394
62	1080
64	360
66	45
68	45

(105, 15, 36) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 34175$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 1405$, $C_6(x) = 4651.7$,
$C_7(x) = 44007$.

i	A_i
0	1
36	5
38	105
40	168
42	695
44	990
46	3030
48	2885
50	6030
52	3705
54	5285
56	2790
58	3915
60	1524
62	1260
64	330
66	160

(90, 15, 30) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 46517$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 21654$, $C_6(x) = 1405$.

i	A_i	i	A_i
0	1	48	2090
30	15	49	1950
31	15	50	1500
32	75	51	1440
33	80	52	1080
34	180	53	720
35	330	54	500
36	330	55	255
37	780	56	225
38	990	57	105
39	1295	58	30
40	1593	59	15
41	1905	60	15
42	2570	63	5
43	1535		
44	2655		
45	2524		
46	2534		
47	2430		

(90, 15, 30) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 1405$.

i	A_i
0	1
30	31
32	135
34	240
36	860
38	2100
40	3498
42	4465
44	5130
46	5175
48	4280
50	3378
52	2040
54	950
56	390
58	45
60	50

(90, 15, 31) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 44007$.

i	A_i	i	A_i
0	1	49	1755
31	30	50	1515
32	90	51	1355
33	150	52	1125
34	105	53	750
35	345	54	595
36	395	55	255
37	450	56	120
38	1065	57	135
39	1295	58	60
40	1668	59	15
41	2325		
42	2520		
43	2325		
44	2520		
45	2496		
46	2460		
47	2700		
48	2145		

(9, 15, 30) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 1405$.

i	A_i
0	1
30	31
32	120
34	345
36	815
38	1905
40	3438
42	4705
44	5370
46	5025
48	4145
50	3243
52	2115
54	1055
56	360
58	75
60	20

(90, 18, 31) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 46517$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 1405$.

i	A_i	i	A_i
0	1	49	1890
31	30	50	1470
32	90	51	1455
33	110	52	1260
34	150	53	885
35	285	54	480
36	470	55	195
37	705	56	90
38	840	57	110
39	1155	58	60
40	1668	59	15
41	2250	60	35
42	2400		
43	2445		
44	2955		
45	2754		
46	2280		
47	2100		
48	2135		

(90, 15, 30) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$; $C_5(x) = 34175$, $C_6(x) = 56300$.

i	A_i
0	1
30	31
32	165
34	225
36	885
38	1830
40	3678
42	4735
44	4935
46	5145
48	4320
50	3333
52	1965
54	1010
56	420
58	75
60	15

(90, 15, 30) Sub-Code

$C_1(x) = 34132$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 46517$.

i	A_i
0	1
30	15
31	45
32	75
33	75
34	105
35	315
36	410
37	765
38	1020
39	1190
40	1770
41	1815
42	2250
43	2730
44	2715
45	2871
46	2610
47	2190
48	1935
50	1668
51	1400
52	1095
53	840
54	415
55	243
56	255
57	120
58	45
59	15

(90, 15, 30) Sub-Code

$C_1(x) = 44007$, $C_2(x) = 46517$, $C_3(x) = 20361$,
$C_4(x) = 21654$, $C_5(x) = 34175$, $C_6(x) = 1405$.

i	A_i
0	1
30	30
32	90
34	375
36	860
38	1770
40	3741
42	4660
44	4860
46	5220
48	4295
50	3465
52	1890
54	1060
56	345
58	60
60	46

(90, 15, 31) Sub-Code

$C_1(x) = 1405$, $C_2(x) = 64272$, $C_3(x) = 20361$,
$C_4(x) = 4274$, $C_5(x) = 34175$, $C_6(x) = 56300$.

i	A_i	i	A_i
0	1	49	1935
31	60	50	
32	75	51	
33	45	52	
34	165	53	
35	303	54	
36	480		
37	615		
38	750		
39	1380		
40	1773		
41	2130		
42	2620		
43	2460		
44	2580		
45	2620		
46	2400		
47	2325		
48	2010		

5.7.3. Sub-Codes derived from (88, 11) Quasi-Cyclic Code.

(77, 11, 31) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1467$, $C_3(x) = 2224$,
$C_4(x) = 1355$, $C_5(x) = 1641$, $C_6(x) = 2547$,
$C_7(x) = 3145$.

i	A_i	i	A_i
0	1	47	33
31	33	49	22
32	55	50	11
33	187	52	11
34	198	55	1
35	165		
36	242		
37	66		
38	44		
39	99		
40	110		
41	253		
42	253		
43	165		
44	77		
46	22		

(77, 11, 30) Sub-Code

$C_1(x) = 1253$, $C_2(x) = 1467$, $C_3(x) = 2224$,
$C_4(x) = 1355$, $C_5(x) = 1541$, $C_6(x) = 2547$,
$C_7(x) = 3145$.

i	A_i
0_1	1
30	11
32	132
34	429
36	363
38	88
40	319
42	462
44	133
46	33
48	44
50	33

(77, 11, 31) Sub-Code

$C_1(x) = 1253$, $C_2(x) = 1467$, $C_3(x) = 2224$,
$C_4(x) = 1355$, $C_5(x) = 1541$, $C_6(x) = 2547$,
$C_7(x) = 2621$.

i	A_i	i	A_i
0	1	47	33
31	44	48	11
32	33	49	22
33	154	50	22
34	242		
35	198		
36	220		
37	55		
38	55		
39	88		
40	121		
41	286		
42	198		
43	132		
44	110		
45	11		
46	11		

(77, 11, 32) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1253$, $C_3(x) = 1467$,
$C_4(x) = 2224$, $C_5(x) = 1355$, $C_6(x) = 1541$,
$C_7(x) = 3145$.

i	A_i
0	1
32	154
34	429
36	341
38	110
40	297
42	462
44	155
46	22
48	44
50	33

(77, 11, 32) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1253$, $C_3(x) = 1467$,
$C_4(x) = 2224$, $C_5(x) = 1355$, $C_6(x) = 2547$,
$C_7(x) = 3145$.

i	A_i
0	1
32	165
34	418
36	330
38	110
40	297
42	484
44	155
46	22
48	33
50	22
52	11

(77, 11, 30) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1253$, $C_3(x) = 2224$,
$C_4(x) = 1355$, $C_5(x) = 1541$, $C_6(x) = 2547$,
$C_7(x) = 3145$.

i	A_i
0	1
30	11
32	110
34	495
36	297
38	110
40	341
42	396
44	199
46	11
48	44
50	33

(77, 11, 30) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1253$, $C_3(x) = 1467$,
$C_4(x) = 2224$, $C_5(x) = 1541$, $C_6(x) = 2547$,
$C_7(x) = 3145$.

i	A_i
0	1
30	11
32	121
34	462
36	330
38	110
40	297
42	462
44	155
46	11
48	77
52	11

(66, 11, 25) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1253$, $C_3(x) = 1467$,
$C_4(x) = 2224$, $C_5(x) = 1355$, $C_6(x) = 3145$.

i	A_i	i	A_i
0	1	44	11
25	33	45	11
26	33		
27	88		
28	121		
29	165		
30	220		
31	121		
32	176		
33	155		
34	143		
35	242		
36	154		
37	110		
38	110		
39	77		
40	33		
41	22		
42	22		

(66, 11, 26) Sub-Code

$C_1(x) = 1547$, $C_2(x) = 2621$, $C_3(x) = 1253$,
$C_4(x) = 1541$, $C_5(x) = 1355$, $C_6(x) = 3145$.

i	A_i
0	1
26	88
28	286
30	385
32	264
34	319
36	363
38	231
40	55
42	33
44	23

(66, 11, 26) Sub-Code

$C_1(x) = 2547$, $C_2(x) = 2621$, $C_3(x) = 1253$,

$C_4(x) = 1467$, $C_5(x) = 1541$, $C_6(x) = 3145$.

i	A_i
0	1
26	121
28	209
30	419
32	297
34	275
36	418
38	187
40	66
42	44
46	11

(66, 11, 26) Sub-Code

$C_1(x) = 2547$, $C_2(x) = 2621$, $C_3(x) = 1253$,
$C_4(x) = 1467$, $C_5(x) = 2224$, $C_6(x) = 3145$.

i	A_i
0	1
26	44
27	143
28	132
29	132
30	209
31	154
32	132
33	155
34	132
35	187
36	198
37	176
38	121
39	44
40	33
41	11
42	22
45	22

(66, 11, 25) Sub-Code

$C_1(x) = 2547$, $C_2(x) = 1253$, $C_3(x) = 1467$,
$C_4(x) = 2224$, $C_5(x) = 1355$, $C_6(x) = 3145$.

i	A_i	i	A_i
0	1	44	11
25	11	45	1.1
26	44		
27	110		
28	121		
29	165		
30	231		
31	175		
32	88		
33	111		
34	175		
35	165		
36	242		
37	198		
38	55		
39	66		
40	33		
42	22		
43	11		

(66, 11, 25) Sub-Code

$C_1(x) = 1541$, $C_2(x) = 2621$, $C_3(x) = 1253$,
$C_4(x) = 1467$, $C_5(x) = 2224$, $C_6(x) = 3145$.

i	A_i
0	1
25	11
26	22
27	121
28	165
29	143
30	187
31	154
32	165
33	166
34	154
35	187
36	121
37	143
38	143
39	44
40	44
41	33
42	22
43	22

(55, 11, 20) Sub-Code

$C_1(x) = 2621$, $C_2(x) = 1253$, $C_3(x) = 1541$,
$C_4(x) = 1467$, $C_5(x) = 3145$.

i	A_i
0	1
20	22
21	77
22	88
23	88
24	165
25	198
26	209
28	253
28	176
29	143
30	154
31	154
32	132
33	56
34	77
35	33
37	22

(55, 11, 20) Sub-Code

$C_1(x) = 2621$; $C_2(x) = 1253$, $C_3(x) = 2547$,
$C_4(x) = 1467$, $C_5(x) = 3145$.

i	A_i
0	1
20	33
21	44
22	99
23	143
24	143
25	198
26	154
27	231
28	198
29	143
30	231
31	132
32	110
33	100
34	44
35	11
36	11
37	11
39	11

(55, 11, 20) Sub-Code

$C_1(x) = 1541$, $C_2(x) = 1253$, $C_3(x) = 2547$,
$C_4(x) = 1467$, $C_5(x) = 3145$.

i	A_i
0	1
20	44
21	55
22	33
23	154
24	198
25	154
26	220
27	209
28	143
29	209
30	209
31	132
32	99
33	56
34	55
35	33
36	11
37	22

CHAPTER 5

CONSTRUCTION OF CONSTANT WEIGHT CODES FROM QUASI-CYCLIC CODES FOR RALEIGH FADING CHANNEL.

5.1 Introduction The use of coding and modulation over Raleigh fading channel is well known. Depending on the specific characteristics of the channel and the expected BER a combination of coding/modulation is designed.

In their paper (14), Pieper et al introduce a novel method of coding/modulation over the noncoherent Raleigh fading channel.

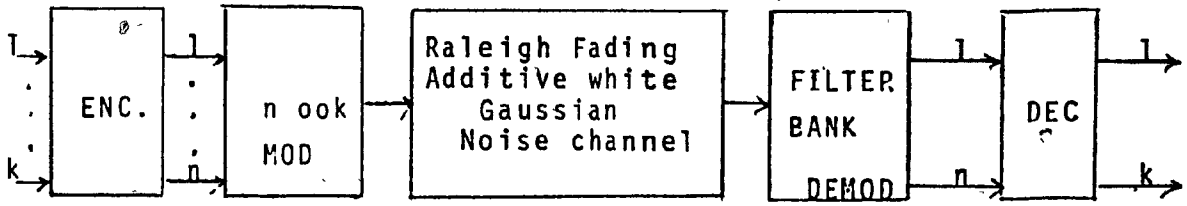


Fig. 5.1 Model of communication channel

The modulator accepts the block of n bits corresponding to a codeword and it assigns each bit to an ook modulator, consequently, there are n ook modulators.

The demodulator we choose here is a sub-optimum decoder using the chase algorithm #2. The received waveform is filtered, the mth filter is matched to the mth ook tone, Since the Raleigh fading and the additive white Gaussian noise are mutually and statistically independent as well as identically distributed

random processes, the maximum likelihood criterion requires that the receiver be composed of "square law envelope detectors". The "target selector" forms the log-likelihood terms for each of the M hypotheses. The codeword corresponding to the maximum of these terms is then selected, (15).

Since we have constant weight code, each codeword has the same amount of energy, the bias term C_i (Wozencraft, page 235) is the same for each codeword, therefore the computation of the log-likelihood quantities is straightforward. Let μ_m be the square of the envelope of the output of the mth matched filter.

It is shown by Gaarder (16) that if the M signal patterns (corresponding to the M codewords) are transmitted with equal a-priori probability then the decoder that achieves the smallest possible probability of error, in choosing the correct codeword based upon the received waveform is the one that computes the M decision variables (log-likelihood quantities) and

$$V_i = \sum_{m=1}^{n} x_{im} |\mu_m|^2 \quad , \; i=1,2,\ldots,M \qquad (5.1)$$

also it is the one that chooses the codeword corresponding to the index i for which the summation is a maximum.

5.2 The construction of constant weight codes from Quasi-Cyclic codes.

As noted on chapter 3 and 5 , some quasi-cyclic codes formed by the normal basis theorem and its sub-codes have interesting weight distribution structures and can be expurgated to form constant weight codes.

We note also that some quasi-cyclic codes formed by the theorem of Seguin (16) have also interesting weight distributions.

Consider now a (n,k,d) binary linear Quasi-cyclic code; by purging the code of all codewords of weight different than those of A_i , the expurgated code (n,k,d) will have the following features

- It is a nonlinear code
- The word size is unchanged
- The number of codewords is equal to or less than A_i, $\log_2 k' \leq A_i$, A_i is the number of codewords of weight i.
- The new minimum distance is at least that of the original code. Therefore $d' \geq d_{min}$, d_{min} is the minimum distance of the original code

Following are some typical Quasi-Cyclic codes which can form powerfull constant weight codes:

(39,13,12) QC code

$C_1 = 1$

$C_2 = 14221$

$C_3 = 13556$

The weight distribution:

A(0) & A(39) = 1

A(12) & A(27) = 156

A(14) & A(24) = 858

A(15) & A(23) = 1053

A(19) & A(20) = 2028

The parameters of the constant weight code are:

Parameters	Original	Constant weight#1	Cons. wgt.#2
n	39	39	39
k	13	10	10
M	8192	2028	1053
d_{min}	12	$\geq$ 12	$\geq$12
W	Variable	19	15
Diversity order*	—	$\geq$6	$\geq$ 6

* see appendix C-1

(52, 13, 16) QC code

C_1 = 1
C_2 = 7715
C_3 = 5477
C_4 = 2767

The weight distribution is :
A (0) & A (52) = 1
A (16) & A (36) = 13
A (20) & A (32) = 1092
A (24) & A (28) = 2990

The parameters of the constant weight code are :

Parameters	Original	Constant weight #1	Constant weight #2
n	52	52	52
k	13	10	11
M	8192	1092	2990
d_{min}	16	$\geq$16	$\geq$16
W	Variable	20	24
Diversity Order*	—	$\geq$8	$\geq$8

* : see appendix C.2

(51, 17, 16) QC code.

C_1 = 1
C_2 = 264626
C_3 = 313151
The weight distribution is :
A(0) & A (51) = 1
A(16) & A (35) = 1530
A(19) & A (32) = 5661
A(20) & A (31) = 8161
A(23) & A (28) = 24480
A(24) & A (27) = 25704

The parameters of the constant weight code are :

Parameters	Original	Constant weight #1	Constant weight #2
n	51	51	51
k	17	14	14
M	131072	24480	25704
d_{min}	16	≥ 16	≥ 16
W	Variable	23	27
Diversity order	—	≥ 8	≥ 8

(91, 13, 36) QC code

C_1 = 1
C_2 = 14221
C_3 = 17227
C_4 = 13006
C_5 = 14771
C_6 = 13556
C_7 = 10550

The weight distribution is

A(0) & A(91) = 1
A(36) & A(55) = 364
A(39) & A(52) = 728
A(40) & A(51) = 546
A(43) & A(48) = 1365
A(44) & A(47) = 1092

The parameters of the constant weight code are:

Parameters	Original	Constant weight #1	Constant weight #2
n	91	91	91
k	13	10	10
M	8192	1365	1092
d_{min}	36	≥ 36	≥ 36
W	Variable	43	44
Diversity order	—	≥ 18	≥ 18

(150, 15, 59) QC code

C_1 = 1405
C_2 = 34175
C_3 = 64272
C_4 = 21654
C_5 = 46517
C_6 = 56300
C_7 = 4274
C_8 = 20361
C_9 = 34132
C_{10} = 44007

The weight distribution is given in chap. 4 , the parameters of the code are :

Parameters	Original	Cons. wgt.#1	Cons. wgt#2	Cons. wgt.#3
n	91	91	91	91
k	13	11	11	11
M	8192	2964	2925	2400
d_{min}	59	$\geq$59	$\geq$59	$\geq$59
W	Variable	75	76	79
Diversity order	—	$\geq$29	$\geq$29	$\geq$29

(88, 11, 39) QC code

C_1 – 1253
C_2 – 1467
C_3 – 2224
C_4 – 1355
C_5 – 1541
C_6 – 2547
C_7 – 2621
C_8 – 3145

The weight distribution is given in chap. 4 , the parameters of the code are :

Parameters	Original	Constant weight#1	Cons. wgt. #2
n	88	88	88
k	11	9	9
M	2048	539	528
d_{min}	39	$\geq$39	$\geq$39
W	Variable	40	47
Diversity order	—	$\geq$18	$\geq$18

(30, 5, 15) QC code

C_1 – 1
C_2 – 11
C_3 – 30
C_4 – 35
C_5 – 26
C_6 – 31

The weight distribution is given in chap. 4, the parameters of the constant weight are :

Parameters	Original	Constant weight #1
n	30	30
k	5	4
M	32	16
d_{min}	15	≥ 15
W	Variable	15
Diversity order	—	≥ 7

5.3 An efficient method of decoding constant weight codes with channel measurement information.

In this section, we are interested in the decoding of constant weight codes derived from quasi-cyclic codes with channel measurement information. The soft decision algorithm used is the Chase algorithm (chapter 4). Let the code composed by s circulants, the transmitted codeword V_m can be expressed as:

$$V_m = \{V_{m1}, V_{m2}, \ldots, V_{mN}\} \qquad (5.2)$$

where V_m has N bits.

Let r_m be the received codeword

$$r_m = \{r_{m1}, r_{m2}, \ldots, r_{mN}\} \qquad (5.3)$$

Associated with the received codeword is the channel measurement sequence α_m

$$\alpha_m = \alpha_{m1}, \alpha_{m2}, \ldots, \alpha_{mN} \qquad (5.4)$$

Let W_v be the weight of the constant weight code sent and W_r be the weight of the received codeword, the number of error bits are equal to $|W_v - W_r|$, therefore

i) If $|W_v - W_r| = 0$, no error is produced or more than d_{min} errors are produced

ii) If $0 < |W_v - W_r| \leq (d_{min}-1)/2$, the error correction can be done solely by the Karlin binary decoder

iii) $(d_{min}-1)/2 < |W_v - W_r| \leq (d_{min}-1)$, there will be as much

$$2^{\{|W_v - W_r| - (d_{min}-1)/2\}} \qquad (5.5)$$

estimations by the Chase algorithm. The Karlin binary decoder will estimate only those $\tilde{e}_i, \tilde{e}_{pc_i}, \tilde{e}_{pc_2}, \ldots, \tilde{e}_{pc(s-1)}$ such that

$$W\{\tilde{e}_i\} + W\{e_{pc_1}\} + \ldots + W\{\tilde{e}_{pc(m-1)}\} = |W_v - W_r| \qquad (5.6)$$

evidently the decoding process can benefit the mechanism of moving into an inner loop as explained in chapter 3.

The estimation is stopped when the set R, (eq. 3.6.5) of test patterns is emptied.

CHAPTER 6

CONCLUSION

6.1 conclusion

In this thesis, we have studied different aspects of Quasi-Cyclic codes.

The weight distribution structures of Quasi-Cyclic codes in systematic and non-systematic forms are studied; Rates 1/2 , 1/3 and 2/3 code are considered in particular. The McWilliams & Sloane identities are found very useful to generate the weight distribution and the minimum distance of the dual code.

The Karlin binary decoder is reviewed for its great practical interest, additionally, it is the only decoding algorithm dedicated to Quasi-Cyclic codes. However, a new dimension, i.e. the channel measurement information, is used to optimize the decoding procedure. The chase algorithm of soft-decision decoding is found to be easily adapted to the Karlin binary decoder where an interactive process between both is developed. Also the concept of "moving into an inner loop" is also developed for the interactive process.

By using the normal basis theorem Quasi-Cyclic codes can be derived from power residue codes. This class of Quasi-Cyclic Codes has very good minimum distance.

(88,11,39) , (150,15,59) Quasi-Cyclic codes are derived. These codes can generate thousands of sub-codes, some of which are quite good. The best of those sub-codes can be compared to the best known codes (linear and nonlinear) listed in McWilliams & Sloane.

Due to their interesting weight distribution structures, some Quasi-Cyclic codes can be expurgated to form constant weight codes. An efficient method of dedoding those new formed codes is developed using a modified Karlin binary decoder with channel measurement information. It is calculated to be faster than the word correlator.

Some topics are left incomplete in this thesis. Here, we generate only some sub-codes of (88,11) , (150,15) quasi-cyclic codes. This still leaves thousands of (88, 11) , (150,15), (112,28) , (126,7) , (240,24) , (256,16) (336,21) , etc... and these may be quite good. We have also observed during the generation of sub-codes that some circulants are good and some are bad, i.e., a bad circulant cannot give the best minimum distance.

An optimal Karlin decoder is devised with channel measurement information. With today's digital processing technology, this can be implemented, with the bank of matched digital filters into a few printed circuit boards. However relatively high speed input, for example greater than 2400 bps, would require bit-slice microcomputer to handle both the decoder as the matched digital filters.

Also, an efficient decoder which is believed to be faster than the word correlator is developed for constant weight codes.

However, these decoding methods need to be constructed or computer simulated to evaluate how fast they are and to compare them to a similar BCH decoder.

Since all of the decoding algorithm can be micro-programmed, good quasi-cyclic codes with a relatively complex decoding algorithm are becoming competitive and are strongly recommended for future decoder design.

REFERENCES

(1) C.T.Long, Elementary Introduction to Number Theory D.C.Health and Company, 1972

(2) E.R.Berlekamp, Algebraic Coding Theory Mc Graw Hill, New York , 1968

(3) W.W.Peterson, Error Correcting Codes MIT Press, Cambridge, MA 1972

(4) R.G.Gallager, Information Theory and Reliable Communication, John Wiley & Sons, Inc 1968 (chapter 5)

(5) C.L.Chen, "Some Results on algebraically structured error correcting codes" Ph. D. dissertation Univ. Hawaii, 1969

(6) J.M.Stein, V.K.Bhargava, S.E.Tavares, "Weight Distribution of some "best" (3m,2m) Binary Quasi-Cyclic codes." IEEE Trans. on Info. Theory, pp 708-711, Nov. 1975

(7) M.Karlin, "Decoding of Circulant Codes" IEEE Trans. on Info. Theory , pp 797-802 Nov. 1970

(8) S.G.S. Shiva & S.E. Tavares, "Decoding a Class of Quasi-Cyclic Codes" I.E.E.C.E., Toronto, CAN Oct 4-6, 1971

(9) E.J.Weldon, Jr., "Decoding binary block codes on q-any output channels." IEEE Trans Info. Theory, 17(1971) , pp 713-718

(10) G.D.Forney, Jr., "Generalized Minimum Distance Decoding" IEEE Trans Info. Theory, 12(1966),pp 125-131

(11) D.Chase, "A Class of algorithms for decoding block codes with Channel Measurement Information." IEEE Trans. Info. Theory, 18(1970), pp 170-182

(12) F.J. McWilliams, N.J.A. Sloane, "The Theory of Error Correcting Codes"
North-Holland publishing company, 1977

(13) C.L. Chen and W.W.Peterson and E.J.Weldon
"Some Results on Quasi-Cyclic Codes"
Inform. Contr., Vol. 15, pp 407-423, Nov. 1969

(14) J.F.Pieper, J.G.Proakis,R.R.Reed and J.K.Wolf
"Design of Efficient Coding and Modulation for a Raleigh Fading Channel", IEEE Inform. Theory 24(1978) pp 457-469 , July 1978

(15) J.M.Wozencraft and I.M.Jacobs, "Principles of communication Engineering.", New York, Wiley 1965

(16) N.T.Gaarder, "Signal design for fast-fading Gaussian Channels"
IEEE Trans. Inform. Theory, Vol.II-17, pp 247-256 May, 1961

(17) V.K.Bhargava, G.E.Séguin and J.M.Stein
"some (mk,k) Cyclic codes in Quasi-Cyclic Form"
IEEE Trans. Inform. Theory, Vol II-24, pp 630-632 September 1978

Appendix C.1

The order of diversity of constant weight code

Let x and y be two codewords of the constant weight code of length n. Define $d_{ij}(x,y)$ for $i,j = 0,1$ as follows:

$d_{00}(x,y)$ = Number of positions in which x has a 0 and y has a 0

$d_{01}(x,y)$ = Number of position in which x has a 0 and y has a 1

$d_{10}(x,y)$ = Number of positions in which x has a 1 and y has a 0

$d_{11}(x,y)$ = Number of positions in which x has a 1 and y has a 1

Note that

$$\left.\begin{aligned} d_{00}(x,y) + d_{01}(x,y) + d_{10}(x,y) + d_{11}(x,y) &= n \\ d_{01}(x,y) + \quad\quad + d_{11}(x,y) &= W(y) \\ d_{10}(x,y) + d_{11}(x,y) &= W(x) \\ d_{01}(x,y) + d_{10}(x,y) &= d_H(x,y) \end{aligned}\right\}$$

For a constant weight code

$$W(x) = W(y) \Rightarrow d_{01}(x,y) = d_{10}(x,y) = \frac{1}{2} d_H(x,y)$$

Therefore, the decision between two codewords x and y, given transmitted, is equivalent to making a binary decision between two hypothesis Hi and Hj. The $d_{10}(x,y)$ terms under Hi are signal plus noise, and under Hj are noise components. The number $d_{10}(x,y)$ is therefore the effective order of diversity of this decision process.

Appendix C.2

Computer program to compute the weight distribution of Quasi-Cyclic Codes.

A computer program was written to compute the weight distribution of (mk,k) quasi-cyclic codes. Under its present form, it can take code length up to 180 bits and informations up to 2^{59} words. However, the code length can be increased by some easy additions on the program, if necessary.

The computing time is quite optimal since a (150,15) code doesn't take more than 3 seconds of computing time. The most time consuming program done up to now is a (87,29) code which takes about 50 to 60 minutes of computing time.

Extensive use of Memory capacity of the CDC 6600 digital computer is made (133,000 words of memory) as a trade-off for computing time.

Large code $k \geq 27$ can be broken down for calculations. For example, calculation of (58,29) code can be broken down to four computer runs where,

1st run starts at information = 0, end at inf.= $2^{27}-1$
2nd run starts at information = 2^{27}, end at inf. = $2^{28}-1$
3rd run starts at information = 2^{28}, end at inf. = $2^{28}+2^{27}-1$
4th run starts at information = $2^{28}+2^{27}$, end at inf. = 2^{29}

For $k < 27$, only one run is necessary.