ON THE DECODING OF BINARY BCH CODES

by

Hsiu Lu Chao

Submitted to the Department of Electrical Engineering in partial fulfilment of the requirements for the degree of

Master of Applied Science

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

September 1972

© Hsiu Lu Chao, Ottawa 1972.

ACKNOWLEDGEMENT

The author wishes to express his thanks to his supervisor Professor S. G. S. Shiva for his patient guidance and to Professors N. U. Ahmed and N. D. Georganas for helpful discussion. Thanks are also due to all those graduate students whose friendship has been of great help throughout the years of this research.

TABLE OF CONTENTS

ABSTRACT

In this thesis we are mainly concerned with the problem of decoding binary Bose-Chaudhuri-Hocquenghem (BCH) codes. We give certain details, which should prove useful in reducing the amount of computation involved in decoding, for codes with small error-correcting capability.

INTRODUCTION

In this introduction we place the concept of error-correcting codes in the context of binary digital communications [1].

Let us consider the system as shown below. The input to the

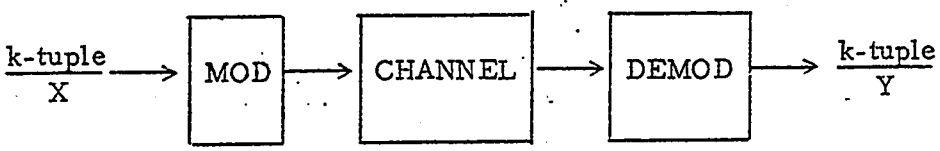

Fig.1

modulator is a message k-tuple X; that is, a sequence of 0's and 1's, there being k bits (binary digits) in all. The 1's correspond to pulses and 0's correspond to no-pulses. Because of the noise in the channel, the output of the channel becomes continuous. The demodulator takes in this channel output and puts out a k-tuple Y. The number e of positions in which X and Y differ is the number of errors. For reliable communication it is clear that e should be small.

As the basic function of the demodulator is to recognize pulse or no-pulse in the presence of noise, one obvious way of reducing e is to increase the signal-to-noise ratio; that is, to make the height of pulse as large as possible with reference to the rms value of the noise.

Another way of reducing e is to have a system as shown below:

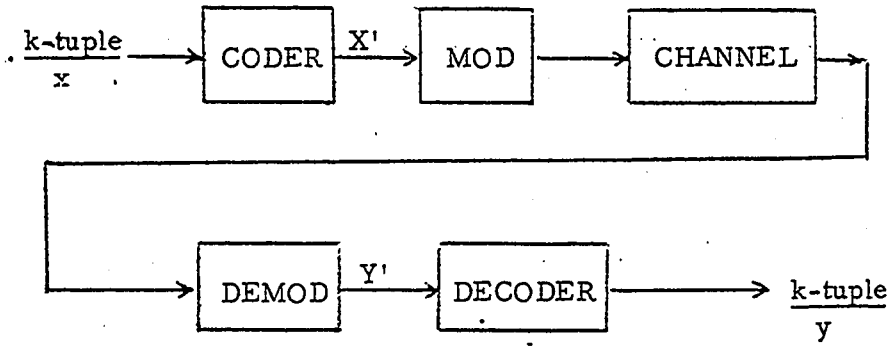

Fig. 2

In this system , the coder takes in the message k-tuple X and transforms this X into an n-tuple X', n > k. The output of the demodulator is an n-tuple Y'. The decoder takes in this Y' and transforms it into a k-tuple Y. If the channel characteristics are such that $e \leq$, say, t, on the average, then the coder and decoder are designed for t. As long as the demodulator does not make more than t errors in n bits, the decoder output Y matches with the input X exactly. In other words, if Y' and X' do not differ in more than t positions, then we have one hundred percent reliable communication.

The set of 2^k message k-tuples is transformed by the coder into a set C of 2^k n-tuples. This set is called an error-correcting code. The code C has 2^k code words each of which is an n-tuple. Since it requires only k-tuples to represent 2^k messages uniquely, out of the n bits, which each code word has, only k bits carry information. Thus k is the number of information bits. The other n-k bits are redundant from the point of view of information. But actually they are the price paid for the error-correcting capability of the code. The ratio k/n, called the information rate, is a measure of the efficiency of the code. For a given error-correcting capability t, we want n to be as small as possible and k/n to be as high as possible. From the discussion so far it is clear that the parameters n=length of the code word, k=number of information bits and t = error-correcting capability are of importance. These parameters are usually written in the form (n, k, t). Thus, for instance, when we say that a certain code is (15, 5, 3), we mean that the code has every word 15 bit long, has 5 information bits and is capable of correcting at most 3 errors in each word.

The type of code under discussion is called a random error correcting code. This means that we have tacitly assumed the channel

to be randomly noisy. On the other hand there are channels which cause the so-called burst errors [2]. In fact there are also channels which cause both random and burst errors. The codes mentioned so far are under the general category of block codes. As opposed to these codes, there are codes like convolutional codes [3]. In this thesis we deal with only random error-correcting block codes.

Among random error-correcting block codes, the so-called BCH codes [4,7] form the largest class. This thesis deals with the problem of decoding [5] BCH codes.

In Chapter I we introduce some of the algebraic concepts which are necessary in dealing with BCH codes.

Chapter II deals with the generation and decoding of BCH codes.

Chapter III is a further discussion on the decoding of BCH codes. The points presented in this chapter simplify the decoding procedure mentioned in Chapter II when t is small.

The thesis ends with certain concluding remarks.

Before concluding this introduction we may mention that, though error-correcting codes have been introduced here in the context of digital communications, these codes have found application in improving the reliability of computing and storage systems [6].

CHAPTER ONE

NECESSARY ALGEBRAIC RESULTS

In this chapter, we mention briefly certain algebraic concepts and results which are necessary for the further development of the thesis. For proofs and details we refer the reader to any standard book on algebra [12] or on the theory of error-correcting codes [1].

A set G of elements, on which one operation ($*$) is defined, is said to be a GROUP if it satisfies the following properties:

(i) Closure.

If a and b belong to G, $a * b$ is in G.

(ii) Associativity.

If a, b and c belong to G, $(a * b) * c = a * (b * c)$.

(iii) Identity.

For every a in G, there exists an identity element e in G such that $a * e = e * a = a$.

(iv) Existence of an inverse.

For all a in G, there exists an element a' in G called the inverse of a such that

$a' * a = a * a' = e$.

A subset of a group is said to be a SUBGROUP if it satisfies all the properties of a group.

A group G is said to be ABELIAN if, for any two elements a and b of G, $a * b = b * a$.

A set R of elements, on which two operations addition (+) and multiplication (.), are defined, is said to be a RING if it satisfies the following properties:

(i) R is an Abelian group under addition.

(ii) Closure.

For all a, b in R, a . b is in R.

(iii) Associativity.

For all a, b, c in R, a . (b . c) = (a . b) . c.

(iv) Distributivity.

For all a, b, c in R;

1. a . (b + c) = a . b + a . c.
2. (b + c). c = b . a + c . a.

A ring R is said to be COMMUTATIVE if, for any two elements a and b of R, a. b = b. a.

A set I of elements is said to be an IDEAL if it is a subgroup of the additive group R and if for every a in R and b in I, ab is in I.

A set F of elements is said to be a FIELD if it is a commutative ring with identity in which every non-zero element has an inverse under multiplication.

In particular, we are interested in a type of fields called GALOIS FIELDS. A Galois Field of 2^q elements is usually denoted by $GF(2^q)$.

Now we discuss the generation of Galois Fields.

Let us consider a POLYNOMIAL $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_r x^r$. Where $a_r = 1$ and every a_i is from GF(2) which consists of the two elements 0 and 1. It is easily verified that 0 and 1 form a field according to the rule $1 + 0 = 0 + 1 = 1$, $0 + 0 = 1 + 1 = 0$, $1 \times 0 = 0 \times 1 = 0 \times 0 = 0$, $1 \times 1 = 1$. In $f(x)$, r is said to be the DEGREE of $f(x)$.

Multiplication, division and addition of polynomials are done as usual except that now all coefficients are computed modulo 2. For instance, $(1 + x) + (x + x^2 + x^3) = 1 + x^2 + x^3$, $\frac{1 + x + x^5}{1 + x + x^2} = 1 + x^2 + x^3$, $(1 + x)(1 + x + x^2 + x^3) = 1 + x^4$.

A polynomial $f(x)$ is said to be IRREDUCIBLE if $f(x)$ cannot be expressed in the form $f(x) = f_1(x) f_2(x)$ where $f_1(x)$ and $f_2(x)$ are over GF(2). Neither $f_1(x)$ nor $f_2(x)$ is trivially unity.

If s is the smallest possible positive integer such that $f(x)$ divides $1 + x^s$, then s is said to be the EXPONENT of $f(x)$.

A polynomial $f(x)$ is said to have α as a ROOT, if $f(\alpha) = 0$.

Let $f(x)$ be irreducible with α as a root. Then all of the roots of $f(x)$ can be expressed as $\alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \ldots, \alpha^{2^{r-1}}$, where the powers are computed modulo s. The set $\{1, \alpha^{2^0}, \alpha^{2^1}, \alpha^{2^2}, \ldots, \alpha^{2^{r-1}}\}$ form a multiplicative group; that is, the set is a group under multiplication.

Let $f(x)$ be irreducible and let β be a root of $f(x)$. Further let $s = 2^q - 1$. Then the set $\{1, \beta, \ldots, \beta^{s-1}\}$ is a GF(2^q) minus the zero element.

For EXAMPLE, suppose $f(x) = 1 + x^3 + x^6$, which is irreducible. Since this $f(x)$ divides $1 + x^9$ and not any $1 + x^p$, $p < 9$, the exponent of $f(x)$ is 9. Suppose β is a root of $f(x)$. Then we have

$$\beta^6 + \beta^3 + 1 = 0,$$

or,

$$\beta^6 = \beta^3 + 1.$$

From this we get,

$$\beta^7 = \beta^4 + \beta,$$

$$\beta^8 = \beta^5 + \beta^2,$$

$$\beta^9 = \beta^6 + \beta^3 = \beta^3 + 1 + \beta^3 = 1.$$

Thus the set $\{1, \beta, \beta^2, \beta^3, \beta^4, \beta^5, \beta^6 = 1 + \beta^3, \beta^7 = \beta^4 + \beta, \beta^8 = \beta^5 + \beta^2\}$ is a multiplicative group. For instance,

$$\beta^5 \cdot \beta^6 = \beta^5 (1 + \beta^3) = \beta^5 + \beta^8 = \beta^5 + \beta^5 + \beta^2 = \beta^2$$

which is again in the set. Note that $\beta^5 \cdot \beta^6 = \beta^{11} = \beta^2$ where 11 modulo 9 = 2.

On the other hand consider the EXAMPLE $f(x) = 1 + x + x^4$ which is known to be irreducible and to have $s = 15 = 2^4 - 1$. Suppose α is a root of $f(x)$. Then

$$\alpha^4 + \alpha + 1 = 0.$$

From this we get the following table,

$$\alpha^0 = \alpha^0,$$

$$\alpha^1 = \alpha^1,$$

$$\alpha^2 = \alpha^2,$$

$$\alpha^3 = \alpha^3,$$

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

$$\alpha^5 = \alpha + \alpha^2,$$

$$\alpha^6 = \alpha^2 + \alpha^3,$$

$$\alpha^7 = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3,$$

$$\alpha^8 = \alpha + \alpha^2 + \alpha^4 = \alpha + \alpha^2 + 1 + \alpha = 1 + \alpha^2,$$

$$\alpha^9 = \alpha + \alpha^3,$$

$$\alpha^{10} = \alpha^2 + \alpha^4 = \alpha^2 + 1 + \alpha = 1 + \alpha + \alpha^2,$$

$$\alpha^{11} = \alpha + \alpha^2 + \alpha^3,$$

$$\alpha^{12} = \alpha^2 + \alpha^3 + \alpha^4 = \alpha^2 + \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^2 + \alpha^3,$$

$$\alpha^{13} = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = \alpha + \alpha^2 + \alpha^3 + 1 + \alpha = 1 + \alpha^2 + \alpha^3,$$

$$\alpha^{14} = \alpha + \alpha^3 + \alpha^4 = \alpha + \alpha^3 + 1 + \alpha = 1 + \alpha^3,$$

$$\alpha^{15} = \alpha + \alpha^4 = \alpha + 1 + \alpha = 1.$$

It is easily verified that the set $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{14}\}$ form a field of $2^4 = 16$ elements. This is a $GF(2^4)$. For instance $\alpha^{12} \cdot \alpha^{13} = \alpha^{25} = \alpha^{10}$ which is in the set. Also, $\alpha^{12} + \alpha^{13} = 1 + \alpha + \alpha^2 + \alpha^3 + 1 + \alpha^2 + \alpha^3 = \alpha$ which is again in the set.

The important difference between the two examples is that while $1 + x^3 + x^6$ can generate only a multiplicative group, $1 + x + x^4$ can generate a $GF(2^4)$.

A binary n-TUPLE is a sequence of 0's and 1's and has n bits.

Hereafter, by an n-tuple we mean a binary n-tuple.

An n-tuple $a_0\, a_1\, a_2 \cdots a_{n-1}$ can be REPRESENTED by the POLYNOMIAL

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

which is over GF(2). Here we note that, in $a_i x^i$, i denotes the position in the sequence and a_i shows the value of the digit in that position.

By a CYCLIC SHIFT of $a_0\, a_1\, a_2 \cdots a_{n-1}$, we mean the sequence $a_{n-1}\, a_0\, a_1\, a_2 \cdots a_{n-2}$. For instance, 100 is a cyclic shift of 001.

By the SUM of two n-tuples $a_0\, a_1\, a_2 \cdots a_{n-1}$ and $b_0 b_1 b_2 \cdots b_{n-1}$, we mean the n-tuple $c_0\, c_1\, c_2 \cdots c_{n-1}$ where $c_i = a_i + b_i$, the addition being modulo 2. In the polynomial representation this means the addition of the coefficients of similar terms modulo 2. For instance, (0 0 0 1 0) + (0 1 1 1 1) = 0 1 1 0 1. In the polynomial representation $(x^3) + (x + x^2 + x^3 + x^4) = x + x^2 + x^4$.

Let C be an additive group such that every element of C is an n-tuple. C is said to be CYCLIC if, for every $a_0\, a_1\, a_2 \cdots a_{n-1}$ in C, the n-tuple $a_{n-1}\, a_0\, a_1 \cdots a_{n-2}$ is also in C. For instance 0 0 0, 0 0 1, 0 1 0, 1 0 0, 0 1 1, 1 1 0, 1 0 1, 1 1 1 is a cyclic C.

It is known that C is cyclic if and only if C is an ideal. This is equivalent to saying that C is cyclic if and only if every element in C is, in the polynomial representation, a multiple of a certain

polynomial $g(x)$ which also belongs to C; that is, every element of C is divisible by $g(x)$. For instance, consider the ideal I generated by $g(x) = 1 + x + x^3$, n being equal to 7. Then every element $C(x)$ of C can be represented by

$$C(x) = (1 + x + x^3)(\lambda_0 + \lambda_1 x + \lambda_2 x^2 + \lambda_3 x^3)$$

where each λ_j is 0 or 1. Thus we have 16 possibilities which constitute C. The elements of C are

0 0 0 0 0 0 0,
0 0 0 1 1 0 1,
1 0 1 0 0 0 1,
1 0 0 1 0 1 1,

1 1 0 1 0 0 0,
1 0 0 0 1 1 0,
1 0 1 1 1 0 0,
1 1 0 0 1 0 1,
0 1 1 0 1 0 0,
0 1 0 0 0 1 1,
0 1 0 1 1 1 0,
1 1 1 0 0 1 0,
0 0 1 1 0 1 0,
0 1 0 0 0 1 1,
0 0 1 0 1 1 1,
0 1 1 1 0 0 1,

It is easily verified that C is cyclic.

This concludes our brief discussion of algebraic results. Further

results will be discussed as they become necessary in later chapters.

The cyclic groups are the basis for all cyclic error-correcting codes. Hence the importance of cyclic groups.

CHAPTER TWO

GENERATION AND DECODING OF BCH CODES

In this chapter we discuss the largest class of random error-correcting codes available. These codes are usually referred to as BCH codes. They were invented by Bose and Chaudhuri [4] on the one hand and by Hocquenghem [7] on the other about the same time. We treat BCH codes as cyclic groups.

In the last chapter we mentioned that cyclic groups could be generated by a generator polynomial $g(x)$. Now we give the rule for choosing $g(x)$ for BCH codes.

An (n, k, t) BCH code V is GENERATED by

$$g(x) = \text{LCM} \{ g_1(x), g_3(x), g_5(x), \ldots, g_{2t-1}(x) \},$$

where each $g_i(x)$ is irreducible and $g_1(x)$ has exponent n, and where if α is a root of $g_1(x)$, then a α^{2i-1} is a root of $g_{2i-1}(x)$. Every code word $V(x)$ can be represented by

$$V(x) = g(x)\ I(x) , \tag{2.1}$$

where $I(x)$ has degree $k - 1$ or less, $V(x)$ has degree $n-1$ or less and $g(x)$ has degree $n-k$. $I(x)$ can be chosen in 2^k ways so that V has 2^k words. The polynomial

$$h(x) = \frac{1 + x^n}{g(x)}$$

has degree k and is called the parity check polynomial.

For EXAMPLE, (15, 5, 3) BCH code can be generated by

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

Here $1 + x + x^4$ has exponent 15. If α is a root of $1 + x + x^4$, we have $1 + \alpha + \alpha^4 = 0$ or $\alpha^4 = 1 + \alpha$. Using the rule $\alpha^4 = 1 + \alpha$, it is easily seen, on computation, that α^3 is a root of $1 + x + x^2 + x^3 + x^4$ and α^5 is a root of $1 + x + x^2$. In this connection we remark that the table of elements of $GF(2^4)$ given in last chapter can be used. In (2 - 1), I(x) is the polynomial representation of the message which is a k-tuple. The polynomial g(x) transforms this I(x) into V(x) which is the polynomial representation of the code word which is an n-tuple. This is an example of the transformation referred to in the Introduction.

Suppose a code word $a_0\, a_1\, a_2 \cdots a_{n-1}$ is passed through a channel and the output is $b_0\, b_1\, b_2 \cdots b_{n-1}$. If b_j is different from a_j, then we say that the channel noise has caused an error in the j^{th} position. Since all sequences are binary and the addition is modulo 2, this means that, if a_j and b_j are complementary, then there is an error in the j^{th} position. This also means that the output sequence $b_0\, b_1\, b_2 \cdots b_{n-1}$ can be treated as the sum of the input sequence $a_0\, a_1\, a_2 \cdots a_{n-1}$ and an error sequence $e_0\, e_1\, e_2 \cdots e_{n-1}$ which is in fact the sum of the input and output sequences. In the error sequence the j^{th} position has a 1 if and only if an error has occurred in that position. For EXAMPLE, if the input is, say, 1 0 1 0 1 and the output is, say, 1 0 0 1 0, then we can say that (1 0 0 1 0) = (1 0 1 0 1)+ (0 0 1 1 1) where (0 0 1 1 1) = (1 0 0 1 0) + (1 0 1 0 1). Here the error sequence is 0 0 1 1 1 and we see that in this sequence 1's occur only in those

places where the input and output sequences differ.

On the basis of the preceding comments we can say that the polynomial R(x) received at the end of the channel can be expressed as

$$R(x) = V(x) + E(x), \qquad (2.2)$$

where V(x) belongs to V and E(x) is the error polynomial. The weight of E(x), indicated by $|E(x)|$, is less than or equal to t; that is, we assume that in the channel not more than t errors can occur per code word.

By the WEIGHT of a polynomial f(x), indicated by $|f(x)|$, we mean the number of nonzero terms in it.

For EXAMPLE, $f(x) = 1 + x + x^8$ has weight 3; that is, $|f(x)| = 3$.

Since g(x) has roots $\alpha, \alpha^3, \alpha^5, \ldots, \alpha^{2t-1}$, and because of (2.1), we get, from (2.2),

$$S_{2i-1} \triangleq R(\alpha^{2i-1}) = E(\alpha^{2i-1}), \; i = 1, 2, \ldots, t. \qquad (2.3)$$

The DECODING PROBLEM is to find E(x), given R(x) or, equivalently, $\{S_1, S_3, \ldots, S_{2t-1}\}$. The set $\{S_1, S_3, \ldots, S_{2t-1}\}$ is called the error SYNDROME since it is unique for each error pattern E(x).

The DECODING PROCEDURE, which was initially given by Peterson [5] and later on refined by Berlekamp [8], Massey [9],

Chien [10] and Burton [11], is basically as follows:

Stage (i). Given R(x), compute the syndrome $\{S_1, S_3, S_5, \ldots, S_{2t-1}\}$. If it turns out to be $\{0, 0, \ldots, 0\}$, then $E(x) = 0$. Otherwise proceed to next stage.

Stage (ii). Using the syndrome in

$$\left.\begin{aligned} S_1^3 + S_3 &= S_1\sigma_2 + \sigma_3, \\ S_1^5 + S_5 &= S_3\sigma_2 + S_2\sigma_3 + S_1\sigma_4 + \sigma_5, \\ S_1^7 + S_7 &= S_5\sigma_2 + S_4\sigma_3 + S_3\sigma_4 + S_2\sigma_5 + S_1\sigma_6 + \sigma_7, \end{aligned}\right\} \quad (2.4)$$

and so on till

$$S_1^{2t-1} + S_{2t-1} = S_{2t-3}\sigma_2 + S_{2t-4}\sigma_3 + \ldots + \sigma_{2t-1},$$

compute the elementary functions $\sigma_2, \ldots, \sigma_t$. We note that $\sigma_1 = S_1$ and that in (2.4) we set $\sigma_j = 0$ for all $j > t$. Also, $S_{2i} = S_i^2$.

It is, of course, possible that (2.4) may have equations which are linearly dependant. In such a case a unique solution is not possible. The way to handle this situation will be discussed in the next chapter.

Stage (iii). Find the roots of the error locator polynomial

$$\sigma(x) = x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \ldots + \sigma_{t-1}x + \sigma_t. \quad (2.5)$$

To continue the EXAMPLE of (15, 5, 3) BCH code, already referred to, suppose

$$R(x) = x^3 + x^5 + x^8.$$

Using the table of the elements of $GF(2^4)$ given in the last chapter, we make the following computations.

With reference to (2. 3), we have

$$S_1 = \alpha^3 + \alpha^5 + \alpha^8,$$

$$S_3 = \alpha^9 + \alpha^{15} + \alpha^{24},$$

$$S_5 = \alpha^{15} + \alpha^{25} + \alpha^{40},$$

which, using the rule $\alpha^4 = 1 + \alpha$, become

$$S_1 = \alpha^3 + (\alpha + \alpha^2) + (1 + \alpha^2) = 1 + \alpha + \alpha^3 = \alpha^7,$$

$$S_3 = \alpha^9 + 1 + \alpha^9 = 1,$$

$$S_5 = 1 + \alpha^{10} + \alpha^{10} = 1.$$

Since the syndrome is not $\{0, 0, 0\}$, $E(x) \neq 0$.

Therefore we compute

$$S_1^3 + S_3 = \alpha^{21} + 1 = \alpha^6 + 1 = \alpha^2 + \alpha^3 + 1 = \alpha^{13},$$

$$S_1^5 + S_5 = \alpha^5 + 1 = \alpha^5 + 1 = \alpha + \alpha^2 + 1 = \alpha^{10}.$$

Using these values in (2-4), we get

$$a^{13} = a^{7}\sigma_2 + \sigma_3,$$

$$a^{10} = \sigma_2 + S_2\sigma_3 = \sigma_2 + S_1^{2}\sigma_3$$

$$= \sigma_2 + a^{14}\sigma_3.$$

Solving these equations, in the same way as we do any set of linear simultaneous equations, for σ_2 and σ_3, we get

$$\sigma_2 = a^{5},$$

$$\sigma_3 = a^{11},$$

Using these two values, we get

$$\sigma(x) = x^{3} + \sigma_1 x^{2} + \sigma_2 x + \sigma_2 x + \sigma_3,$$

$$= x^{3} + a^{7}x^{2} + a^{5}x + a^{11}.$$

Setting $x = a^{0}, a^{1}, a^{2}, \ldots$, in turn, in $\sigma(x)$, we find that $\sigma(a^{3}) = 0$, $\sigma(a^{5}) = 0$, $\sigma(a^{10}) = 0$. Therefore $E(x) = x^{5} + x^{8} + x^{10}$.

The decoding procedure discussed in this chapter is applicable to all BCH codes. There are simpler decoding procedures like threshold decoding [3] and permutation decoding (error trapping) [2]. But not all BCH codes can be decoded by these simpler procedures. Some of the BCH codes, which are majority logic decodable or threshold decodable, are mentioned in the literature [3]. We do

not discuss these simpler procedures.

The Stage (ii) of the decoding procedure, as already mentioned, is finding σ_j's from (2.4). In this connection Berlekamp's algorithm [8] as well as Massey's [9] "physical interpretation" can be very effectively used.

In regard to Stage (iii), the Chien search [10] can be used to find the roots of $\sigma(x)$ speedily.

With reference to Stage (iii), the following observation, made by Chien [10], is also extremely useful. Let us consider the error locator polynomial (2.5) which is rewritten here for the sake of convenience:

$$\sigma(x) = x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \ldots + \sigma_{t-1} x + \sigma_t .$$

If some of σ_i's are zero, the amount of computation involved in finding the roots of $\sigma(x)$ is reduced. Even when $\sigma_1, \sigma_2, \ldots, \sigma_{t-1}$ are all not zero, it is possible to find a γ under certain conditions, such that in the polynomial $\rho(y)$, obtained by setting $x = y + \gamma$ in $\sigma(x)$, one term is missing. From the point of view of the amount of computation involved, it is easier to find the roots of $\rho(y)$ than $\sigma(x)$.

Further comments on Stages (ii) and (iii) will be made in the next chapter.

CHAPTER 3

FURTHER DISCUSSION ON DECODING BCH CODES

In this chapter we give details regarding the decoding procedure discussed in the previous chapter. These details should be helpful in implementing the procedure.

3.10 Finding the Elementary Functions

As already stated in Chapter 2, the Stage (ii) of the decoding procedure involves solving

$$S_1^3 + S_3 = S_1\sigma_2 + \sigma_3,$$

$$S_1^5 + S_5 = S_3\sigma_2 + S_2\sigma_3 + S_1\sigma_4 + \sigma_5,$$

$$S_1^7 + S_7 = S_5\sigma_2 + S_4\sigma_3 + S_3\sigma_4 + S_2\sigma_5 + S_1\sigma_6 + \sigma_7,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$S_1^{2t-1} + S_{2t-1} = S_{2t-3}\sigma_2 + S_{2t-4}\sigma_3 + S_{2t-5}\sigma_4 + \ldots + \sigma_{2t-1}.$$

for the elementary functions $\sigma_2, \sigma_3, \ldots, \sigma_t$. Here $\sigma_j = 0$ for $j>t$.

The equations (3-1) are the same as (2-4). They have been written here again for the sake of convenience. Also, we note that $\sigma_1 = S_1$.

In (3-1) there are t-1 equations and t-1 unknowns. The equations can be rewritten in the matrix form

$$M_t \begin{bmatrix} \sigma_2 \\ \sigma_3 \\ \cdot \\ \cdot \\ \cdot \\ \sigma_t \end{bmatrix} = P_t, \qquad (3\text{-}2)$$

where M_t is a (t-1)-by-(t-1) matrix with S_i's as entries and P_t is a column matrix.

It is known[8]that the determinant of M_t, indicated by Δ_t, is zero if and only if the actual number e of errors that have occured is less than t-1. In other words the error locator polynomial

$$\sigma(x) = x^t + \sigma_1 x^{t-1} + \sigma_2 x^{t-2} + \ldots + \sigma_{t-1} x + \sigma_t \qquad (3\text{-}3)$$

has one or more repeated roots if and only if $\Delta_t = 0$. If $e = t - 1$, then $\Delta_t \neq 0$, but σ_t will turn out to be zero.

If $\Delta_t = 0$, then we know $e \leq t-2$. Therefore we form, parallel to (3-3),

$$M_{t-2} \begin{pmatrix} \sigma_2 \\ \sigma_3 \\ \cdot \\ \cdot \\ \cdot \\ \sigma_{t-2} \end{pmatrix} = P_{t-2}, \qquad (3-4)$$

by taking the first t-3 equations from (3-1) and setting $\sigma_{t-1} = \sigma_t = 0$. If $\Delta_{t-2} = 0$, then $e \leq t-4$ and we repeat the process.

This means that we are interested in the determinant Δ_{t-2i_0} such that Δ_{t-2i_0} is nonzero and that Δ_{t-2i} is zero for all $i < i_0$. Setting $t' = t - 2i_0$, we have $e = t'$ or $t'-1$. Here Δ_{t-2i_0} is the determinant of the matrix $M_{t'}$ formed by taking the first $t'-1$ equations from (3-1) and setting $\sigma_{t'+1} = \sigma_{t'+2} = \cdots = \sigma_t = 0$ in the equations. In the error locator polynomial

$$\sigma(x) = x^{t'} + x^{t'-1}\sigma_1 + x^{t'-2}\sigma_2 + \cdots + \sigma_{t'}$$

$\sigma_1, \sigma_2, \ldots, \sigma_{t'}$ are as determined from the first t'-1 equations.

The method described is the traditional way of determining the elementary functions. Compared to this method, the Berlekamp's algrithm is faster. However, when t is small, the traditional method can be used effectively by breaking the Stage (ii) into substages This aspect will be demonstrated for t's up to 5.

In the context of the preceding comments let us consider Δ_i for i = 3, 4, 5. We have, with reference to (3-1),

$$\Delta_3 = \begin{vmatrix} S_1 & 1 \\ S_3 & S_2 \end{vmatrix} = S_3 + S_1^3, \qquad (3\text{-}5)$$

$$\Delta_4 = \begin{vmatrix} S_1 & 1 & 0 \\ S_3 & S_2 & S_1 \\ S_5 & S_4 & S_3 \end{vmatrix} = S_3\Delta_3 + S_4 \begin{vmatrix} S_1 & 0 \\ S_3 & S_2 \end{vmatrix}$$

$$+ S_5 \begin{vmatrix} 1 & 0 \\ S_2 & S_1 \end{vmatrix}$$

$$= S_3\Delta_3 + S_1(S_1^5 + S_5), \qquad (3\text{-}6)$$

$$\Delta_5 = \begin{vmatrix} S_1 & 1 & 0 & 0 \\ S_3 & S_2 & S_1 & 1 \\ S_5 & S_4 & S_3 & S_2 \\ S_7 & S_6 & S_5 & S_4 \end{vmatrix}$$

$$= S_4\Delta_4 + S_5(S_5 + S_2S_3) + S_6S_1(S_3 + S_1^3) + S_7(S_1^3 + S_3)$$

$$= S_4\Delta_4 + (S_1^3 + S_3)(S_1S_6 + S_7) + S_5(S_5 + S_2S_3)$$

$$= S_4\Delta_4 + \Delta_3(S_1S_6 + S_7) + S_5(S_5 + S_2S_3), \qquad (3\text{-}7)$$

which can also be rewritten as

$$\Delta_5 = S_4\left[S_3\Delta_3 + S_1(S_1^5 + S_5)\right] + \Delta_3(S_1S_6 + S_7) + S_5(S_5 + S_2S_3)$$

$$= \Delta_3(S_3S_4 + S_1S_6 + S_7) + S_1^5(S_1^5 + S_5) + S_5(S_5 + S_2S_3)$$

$$= \Delta_3\left[S_1S_3(\Delta_3) + S_7\right] + (S_1^5 + S_5)^2 + S_1^5S_5 + S_5S_2S_3$$

$$= S_1S_3\Delta_3^2 + \Delta_3S_7 + (S_1^5 + S_5)^2 + S_5S_1^2\Delta_3$$

$$= S_1S_3\Delta_3^2 + (S_1^2S_5 + S_7)\Delta_3 + (S_1^5 + S_5)^2. \qquad (3\text{-}7a)$$

The expressions (3-5), (3-6), (3-7) will now be used to analyse the cases of t = 3, 4 and 5. The cases of t = 1, and t = 2 have been dealt with in detail in literature, and do not need any elaboration here. Still, for the sake of completeness, we consider these two cases also.

3.11 Case of t = 1

(i) $\{ S_1 = 0 \} \Longleftrightarrow \{ E(x) = 0 \}$.

(ii) $\{ S_1 \neq 0 \} \Longleftrightarrow \{ E(x) = x^a$, where a is given by $S_1 = \sigma_1 = \alpha^a \}$.

3.12 Case of t = 2

(i) $\{S_1 = 0\} \Longleftrightarrow \{E(x) = 0\}$.

The proof is as follows : $\{S_1 = 0\} \Longrightarrow \{|E(x)| = 0 \text{ or} \geq 3\}$. But $E(x) \not> 2$. Therefore $E(x) = 0$. The converse is obvious.

(ii) $\{S_1^3 = S_3\} \Longleftrightarrow \{E(x) = x^a$, where a is given by $S_1 = \sigma_1 = \alpha^a\}$.

The proof is as follows : From (3-1),

$$\sigma_2 = \frac{S_1^3 + S_3}{S_1}.$$

Therefore $\{S_1^3 = S_3\} \Longrightarrow \{\sigma_2 = 0\} \Longrightarrow \{E(x) = x^a\}$. The converse is obvious.

(iii) $\{S_1^3 \neq S_3\} \Longleftrightarrow \{|E(x)| = 2\}$.

Since the situations of $|E(x)| = 0$ and $|E(x)| = 1$ have already been taken care of , (iii) is obvious. E(x) is determined by finding the roots of

$$\sigma(x) = x^2 + S_1 x + \frac{S_1^3 + S_3}{S_1}.$$

3.13 Case of t = 3

(i) $\left\{S_1 = 0,\ S_3 = 0\right\} \Longleftrightarrow \left\{E(x) = 0\right\}$.

The proof lies in the fact that $\left\{S_1 = 0,\ S_3 = 0\right\} \Longrightarrow \left\{|E(x)| \geq 5 \text{ or } 0\right\}$. But $|E(x)| \leq 3$. Therefore $E(x) = 0$. The converse is obvious.

(ii) $\left\{S_3 = S_1^3\right\} \Longleftrightarrow \left\{E(x) = x^a, \text{ where a is given by } S_1 = \sigma_1 = a^a\right\}$.

The proof is as follows : From Δ_3, $\left\{S_3 = S_1^3\right\} \Longrightarrow \left\{\text{a repeated root}\right\}$. Therefore $|E(x)| < t\text{-}1 = 2$. But $E(x) \neq 0$ because of (i). Hence $|E(x)| = 1$. The converse is obvious.

(iii) Solving (3-1) we get

$$\sigma_2 = \frac{S_1^2 S_3 + S_5}{S_1^3 + S_3},$$

$$\sigma_3 = S_1\sigma_2 + S_1^3 + S_3.$$

Using these σ_2 and σ_3 in

$$\sigma(x) = x^3 + S_1x^2 + \sigma_2 x + \sigma_3,$$

we find the roots of $\sigma(x)$ and get $E(x)$ from these roots.

3.14 Case of t = 4

(i) $\{ S_1 = 0, S_3 = 0 \} \Longleftrightarrow \{ E(x) = 0 \}$.

The proof lies in the fact that $\{ S_1 = 0, S_3 = 0 \} \Longrightarrow \{ |E(x)| = 0 \text{ or } \geq 5 \}$. But $|E(x)| \leq 4$. Therefore $E(x) = 0$. The converse is obvious.

(ii) $\{ S_3(S_3 + S_1^3) + S_1(S_1^5 + S_5) = 0 \} \Longrightarrow \{ |E(x)| = 1 \text{ or } 2 \}$.

From (3-5), $\{ S_3(S_3 + S_1^3) + S_1(S_1^5 + S_5) = 0 \} \Longrightarrow \{ \text{repeated root} \}$. Then $|E(x)| < t-1 = 3$; that is $|E(x)| = 0, 1 \text{ or } 2$. We note that (i) has taken care of the situation $E(x) = 0$. Hence $|E(x)| = 1$ or 2. Thus we have now the case of $t = 2$.

(iii) Now we are left with the situation of $|E(x)| = 3$ or 4. From (3-1) we get

$$\sigma_2 = \frac{S_3S_5 + S_1S_7 + S_1^2S_3(S_3 + S_1^3)}{\Delta_4},$$

$$\sigma_3 = S_1^3 + S_3 + S_1\sigma_2,$$

$$\sigma_4 = \frac{S_1^2 S_3 + S_5 + \sigma_2(S_1^3 + S_3)}{S_1} \text{ or } \frac{S_7 + S_1^4 S_3 + \sigma_2(S_1^5 + S_5)}{S_3}.$$

The expression for σ_2 is valid since the case of $\Delta_4 = 0$ is covered in (ii). That for σ_3 is obviously valid. In the cases of the expressions for σ_4, at least one of them should be valid since S_1 and S_3 can not both be zero simutaneously because of (i). We compute the values of σ_2, σ_3, and σ_4 from these expressions and construct

$$\sigma(x) = x^4 + \sigma_1 x^3 + \sigma_2 x^2 + \sigma_3 x + \sigma_4.$$

We find the roots of $\sigma(x)$ and thereby get $E(x)$.

3.15 Case of t = 5

(i) $\{S_1 = 0, S_3 = 0, S_5 = 0\} \Longleftrightarrow \{|E(x)| = 0 \text{ or } \geq 7\}$.

But $|E(x)| \leq 5$. Hence $E(x) = 0$. The converse is obvious.

(ii) $\left\{S_1^3 = S_3,\ S_1^5 = S_5,\ S_1^7 = S_7,\ S_1^9 = S_9\right\} \Longleftrightarrow \left\{E(x) = x^a,\ \text{where } a \text{ is given by } S_1 = \alpha^a\right\}$.

The proof is as follows : Setting $S_1^3 = S_3$, $S_1^5 = S_5$, $S_1^7 = S_7$ and $S_1^9 = S_9$ in (3-1), we get

$$0 = S_1\sigma_2 + \sigma_3, \tag{3-8}$$

$$0 = S_1^3\sigma_2 + S_1^2\sigma_3 + S_1\sigma_4 + \sigma_5.$$

Combining these two equations we get

$$S_1\sigma_4 + \sigma_5 = 0. \tag{3-9}$$

Thus we have the two conditions (3-8) and (3-9). Using them, we have

$$\begin{aligned}\sigma(x) &= x^5 + \sigma_1 x^4 + \sigma_2 x^3 + \sigma_3 x^2 + \sigma_4 x + \sigma_5 \\ &= x^5 + \sigma_1 x^4 + \sigma_2 x^3 + \sigma_1\sigma_2 x^2 + \sigma_4 x + \sigma_1\sigma_4 \\ &= x^2\left\{x(x+\sigma_1) + \sigma_2(x+\sigma_1)\right\} + \sigma_4(x+\sigma_1) \\ &= x^2(x+\sigma_1)(x^2+\sigma_2) + \sigma_4(x+\sigma_1) \\ &= (x+\sigma_1)\left\{x^2 + x\sqrt{\sigma_2} + \sqrt{\sigma_4}\right\}^2,\end{aligned}$$

where it means that $\sigma(x)$ has two roots each of which is repeated twice. Thus $|E(x)| = 1$. The converse is obvious.

(iii) $\left\{\Delta_5 \text{ of } (3\text{-}6) = 0\right\} \Longleftrightarrow \left\{|E(x)| = 2 \text{ or } 3\right\}$.

$\left\{\Delta_5 \text{ of } (3\text{-}6) = 0\right\} \Longleftrightarrow \left\{|E(x)| = 1, 2 \text{ or } 3\right\}$. But the case of $|E(x)| = 1$ has already been covered in (ii). Therefore $|E(x)| = 2$ or 3. Thus we have (iii) of the case of $t = 3$.

(iv) Now the remaining situations are $e = 4$ or 5.

We compute $\sigma_2, \sigma_3, \sigma_4, \sigma_5$ from

$$\sigma_2 = \frac{S_9\Delta_3 + \Delta_3^4 + S_7(S_1^5 + S_5) + S_5S_1^2(S_2S_3 + S_5)}{\Delta_5},$$

$$\sigma_3 = S_1^3 + S_3 + S_1\sigma_2,$$

$$\sigma_4 = \frac{S_2(S_1^5 + S_5) + (S_1^7 + S_7) + (S_2S_3 + S_5)\sigma_2 + (S_2^2 + S_4)\sigma_3}{(S_1S_2 + S_3)},$$

or

$$\sigma_4 = \frac{S_4(S_1^5 + S_5) + (S_1^9 + S_9) + (S_4S_3 + S_7)\sigma_2 + (S_4S_2 + S_5)}{(S_1S_4 + S_5)}$$

$$\sigma_5 = S_1^5 + S_5 + S_3\sigma_2 + S_2\sigma_3 + S_1\sigma_4,$$

which expressions are derived from (3-1).

In these expressions $\Delta_5 \neq 0$ since the case of Δ_5 has been taken care of in (iii). Suppose $S_1^3 = S_3$ and $S_1^5 = S_5$. Then from the first two equations in (3-1), we have $S_1\sigma_2 + \sigma_3 = 0$ and $S_1\sigma_4 + \sigma_5 = 0$. Using all these conditions obtained so far on the right hand side of the fourth equation in (3-1), we get the right hand to be zero so that $S_1^9 = S_9$. Thus we have $S_1^3 = S_3$, $S_1^5 = S_5$, $S_1^7 = S_7$, $S_1^9 = S_9$, all of which mean from (i) that $|E(x)| = 1$. Hence $S_1^3 = S_3$ and $S_1^5 = S_5$ can not be simutaneously valid. Therefore, at least one of the two expressions for σ_4 must be valid. So we have shown that the expressions for $\sigma_2, \sigma_3, \sigma_4$ and σ_5 are valid.

3.16 Example

Let us consider the (15, 1, 4) BCH code generated by

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

This code is trivial in the sense that the information rate k/n is only 1/15. However, this does not affect the illustration of decoding procedure. Suppose $E(x) = x^5 + x^{12}$. Then using the $GF(2^4)$ given in Chapter 1, we have

$$S_1 = E(\alpha) = \alpha^5 + \alpha^{12} = \alpha + \alpha^2 + 1 + \alpha + \alpha^2 + \alpha^3 = 1 + \alpha^3 = \alpha^{14},$$

$$S_3 = E(\alpha^3) = \alpha^{15} + \alpha^6 = 1 + \alpha^2 + \alpha^3 = \alpha^{13},$$

$$S_5 = E(\alpha^5) = \alpha^{10} + 1 = 1 + \alpha + \alpha^2 + 1 = \alpha^5,$$

$$S_7 = E(\alpha^7) = \alpha^5 + \alpha^9 = \alpha + \alpha^2 + \alpha + \alpha^3 = \alpha^6.$$

The problem now is to get $\sigma(x)$, given that $S_1 = \alpha^{14}$, $S_3 = \alpha^{13}$, $S_5 = \alpha^5$, $S_7 = \alpha^6$.

With reference to the case of $t = 4$, we note that (i) is not valid. Regarding (ii) we have

$$\begin{aligned}
\Delta_4 &= S_3(S_1^3 + S_3) + S_1(S_1^5 + S_5) \\
&= \alpha^{13}(\alpha^{12} + \alpha^{13}) + \alpha^{14}(\alpha^5 + \alpha^{10}) \\
&= \alpha^{13}(1 + \alpha + \alpha^2 + \alpha^3 + \alpha^2 + 1 + \alpha^3) + \alpha^{14}(\alpha^5 + \alpha^{10}) \\
&= \alpha^{13}(\alpha) + \alpha^{14}(\alpha + \alpha^2 + 1 + \alpha + \alpha^2) \\
&= \alpha^{14} + \alpha^{14} \\
&= 0.
\end{aligned}$$

Therefore $|E(x)| = 1$ or 2. With reference to the 3.12 Case of $t = 2$, (ii) is not valid. Hence $|E(x)| = 2$. From (iii), we have

$$\sigma(x) = x^2 + S_1 x + \frac{S_1^3 + S_3}{S_1} = x^2 + \alpha^{14} x + \alpha^2.$$

The roots of this can be verified to be α^5 and α^{12}.

3.17 General Comments

From the discussion so far it is clear that, for a given t, if we can store the expressions for $\sigma_2, \sigma_3, \ldots, \sigma_t$ for the case of t, the expressions for $\sigma_2, \sigma_3, \ldots, \sigma_{t-2}$ for the case of t-2, the expressions for $\sigma_2, \sigma_3, \ldots, \sigma_{t-4}$ for the case of t-4 and so on, finding the elementary functions for any situation $e \leq t$ is not difficult. When t is small, the storing of these expressions is quite practical. Furthermore, the amount of storing can be reduced by recognizing the fact that expressions like $S_1^3 + S_3$ which occur so often need be stored only once. Also, it is clear from (3-1) that really we have to get the expressions for only $\sigma_2, \sigma_4, \sigma_6$ and so on, since expressions for σ_3, σ_5 and so on are simply linear combinations of $\sigma_2, \sigma_4, \sigma_6$ and so on.

It can be verified that solving the example of 3.1 by the Berlekamp's algorithm takes much more computation than what was used here.

However, when t is large, Berlekamp's algorithm would be more practical and should therefore be used. In this connection, the Burton modification [11] is also useful.

Some of the conditions mentioned in Sections 3.11 to 3.15 are quite general in fact. In this regard we give the following points.

(i) $\left\{ S_1 = 0,\ S_3 = 0,\ \ldots,\ S_{2i-1} = 0,\ S_{2i+1} \neq 0 \right\} \Longrightarrow \left\{ |E(x)| \geq 2i+1 \right\}$.

(ii) $\left\{ S_1 = 0,\ S_3 = 0,\ \ldots,\ S_{t-2} = 0,\ S_t \neq 0 \right\} \Longrightarrow \left\{ |E(x)| = t \right\}$, if t is odd ≥ 3.

(iii) $\left\{ S_1 = 0,\ S_3 = 0,\ S_5 = 0,\ \ldots,\ S_{t-1} = 0 \right\} \Longrightarrow \left\{ E(x) = 0 \right\}$, if t is even.

(iv) $\left\{ S_1 = 0,\ S_3 = 0,\ \ldots,\ S_t = 0 \right\} \Longleftrightarrow \left\{ E(x) = 0 \right\}$, if t is odd.

The proofs of (i), (ii), (iii) and (iv) are based on the fact that for every word of an i-error-correcting code $S_1 = 0,\ S_3 = 0,\ \ldots,\ S_{2i-1} = 0$.

(v) $\left\{ S_1^3 = S_3,\ S_1^5 = S_5,\ \ldots,\ S_1^{2t-1} = S_{2t-1} \right\} \Longleftrightarrow$ $\left\{ E(x) = x^a, \text{ where a is given by } S_1 = \alpha^a \right\}$.

The proof of (v) is as follows : In view of the first equation of (3-1), $\left\{ S_1^3 = S_3 \right\} \Longrightarrow \left\{ S_1\sigma_2 + \sigma_3 = 0 \right\} \Longrightarrow \left\{ S_1^3\sigma_2 + S_1^2\sigma_3 = S_3\sigma_2 + S_2\sigma_3 = 0 \right\}$. Further in view of the second equation of (3-1),

$\left\{ S_3\sigma_2 + S_2\sigma_3 = 0,\ S_1^5 = S_5 \right\} \Longrightarrow \left\{ S_1\sigma_4 + \sigma_5 = 0 \right\} \Longrightarrow$ $\left\{ S_1^2 S_1\sigma_4 + S_1^2\sigma_5 = S_3\sigma_4 + S_2\sigma_5 = 0 \right\}$. Continuing this argument we get $S_1\sigma_2 = \sigma_3$, $S_1\sigma_4 = \sigma_5$, and so on till $S_1\sigma_{t-1} = \sigma_t$ if t is odd. If t is even, $\sigma_t = 0$. Therefore, defining $t' = t$ if t is odd and $t' = t-1$ if t is even,

$$\sigma(x) = x^{t'} + \sigma_1 x^{t'-1} + \sigma_2 x^{t'-2} + \sigma_3 x^{t'-3} + \ldots + \sigma_{t'}$$

$$= x^{t'} + \sigma_1 x^{t'-1} + \sigma_2 x^{t'-2} + \sigma_1\sigma_2 x^{t'-3} + \ldots + \sigma_1\sigma_{t'-1}$$

$$= (x + \sigma_1) \left\{ x^{t'-1} + \sigma_2 x^{t'-3} + \ldots + \sigma_{t'-1} \right\} ,$$

where every term in the flower brackets is even powered, since t' is even. Therefore every root of $\sigma(x)$ execpt for σ_1 occurs an even number of times. Hence $E(x) = x^a$. The converse is obvious.

3.18 Even Weighted Codes

Let us consider the subset V' of (n, k, t) BCH code V such that V' is made up of all of the words, of V, having even weight. As can be easily shown, V' is cyclic and can be treated as being generated by the polynomial of $g'(x) = g(x)(1 + x)$ where g(x) is the generator polynomial of V. Thus V' is (n,k-1) compared to V. V' has only one information bit less. The error correcting capability of V' is the same as that of V. Thus, V' is (n,k-1,t) and is practically as good as V. With

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

where V'(x) belongs to V' and $|E(x)| \leq t$, we note that

(i) $\left\{ |R'(x)| \text{ odd} \right\} \Longleftrightarrow \left\{ |E(x)| \text{ odd} \right\}$,

(ii) $\{|R'(x)| \text{ even}\} \Longleftrightarrow \{|E(x)| \text{ even}\}$.

The proofs of (i) and (ii) follow from the simple fact that if A_1 and A_2 are two n-tuples, then $|A_1 + A_2|$ is odd if A_1 and A_2 are even(odd) and odd(even) respectively and $|A_1 + A_2|$ is even if A_1 and A_2 are both odd or even.

Because of (i) and (ii), the decoding of V' is a little simpler than that of V' in the following sense : Suppose t is even (odd). Under this condition, if $|R(x)|$ is odd (even), then e is odd (even), then e is odd (even) and at most t-1. This means that in the decoding procedure we have to deal with Δ_{t-1}, Δ_{t-3} and so on, whereas in the case of V we always have to deal with Δ_t, Δ_{t-2}, and so on. Since in the case of V there is no way of knowing a priori whether e is odd or even. We note that Δ_{t-1}, Δ_{t-3} and so on are simpler expressions than Δ_t, Δ_{t-2}, and so on, and consequently involve less computation.

This is one advantage in using V' rather than V. There are also other advantages.

3.20 Finding Roots of Error Locator Polynomial

As stated in the previous chapter, the Stage (iii) of the decoding

procedure is to find the roots of the error locator polynomial. If $\Delta_t = \Delta_{t-2} = \ldots = \Delta_{t-2i} = 0$ and $\Delta_{t-2(i+1)} \neq 0$, then $e = t' = t - 2(i+1)$ or $e = t'-1$. Therefore $\sigma_2, \sigma_3, \ldots, \sigma_{t'}$ are determined from the first $t'-1$ equations of (3-1), taking $\sigma_j = 0$ for $j>t'$; that is, we treat the situation as an t'-error correcting code. So, what we are interested in are the roots of the polynomial

$$\sigma(x) = x^{t'} + \sigma_1 x^{t'-1} + \sigma_2 x^{t'-2} + \ldots + \sigma_{t'-1} x + \sigma_{t'}.$$

We note that $\sigma(x)$ has no repeated roots. If $\sigma_{t'}$ turns out to be zero, then $e = t' - 1$ so that $\sigma(x)$ would become

$$\sigma(x) = x^{t'-1} + \sigma_1 x^{t'-1} + \sigma_2 x^{t'-2} + \ldots + \sigma_{t'-1}.$$

For the sake of convenience in expression let us write down $\sigma(x)$ in the form

$$\sigma(x) = x^{e} + \sigma_1 x^{e-1} + \sigma_2 x^{e-2} + \ldots + \sigma_{e-1} x + \sigma_e,$$

where $\sigma_e \neq 0$.

Basicly the way to find the roots of $\sigma(x)$ is to compute $\sigma(\alpha^j)$, $j = 0, 1, 2$ and so on, and see for what values of j the quantity $\sigma(\alpha^j)$ becomes zero. It is clear that for every $\sigma_j = 0$ the amount of computation is reduced by a certain amount. In this regard the worst situation is

when no σ_j is zero. Next we will show that even in this situation we can reduce the computation by simple transformations.

3.21 Case of e odd

Let $\rho(y)$ be the polynomial obtained by setting $x = y + \sigma_1$ in $\sigma(x)$. Then, in $\rho(y)$, the term y^{t-1} is missing.

The proof of this statement is as follows : If we set $x = y + \phi$ in $\rho(x)$, then the coefficient of y^{e-1} will be $e\phi + \sigma_1$. Here $e = 1$ since e is odd. Clearly $\phi + \sigma_1 = 0$ if we make $\phi = \sigma_1$.

3.22 Case of e = 4m

Let $\rho(y)$ be the polynomial obtained by setting $x = y + \frac{\sigma_2}{\sigma_1}$ $\rho(x)$. Then, in $\rho(y)$, the term y^{t-2} is missing.

The proof of this statement is as follows: Setting $x = y + \phi$ in $\sigma(x)$ we find the coefficient of y^{t-2} to be

$\frac{e(e-1)}{2}\phi^2 + \sigma_1(e-1) + \sigma_2$. Here $\frac{e(e-1)}{2}$ is even since e is a multiple of 4, and therefore $\frac{e(e-1)}{2} = 0$. On the other hand $e-1 = 1$ since e-1 is odd. Thus if $\phi = \frac{\sigma_2}{\sigma_1}$, then the entire coefficient becomes zero. Consequently y^{t-2} is missing in $\rho(y)$.

3.23 Case of e = 2m, m odd, and $\sigma_1 = 0$

Let $\rho(y)$ be the polynomial obtained by setting $x = y + \sqrt{\sigma_2}$ in $\sigma(x)$. Then the terms y^{t-1} and y^{t-2} are missing in $\rho(y)$. The proof of this statement is as follows : Setting $x = y + \phi$ in $\sigma(x)$ we find the coefficient of y^{t-1} to be $\phi e + \sigma_1$. If $\sigma_1 = 0$ and e even, then this coefficient becomes zero. If $\sigma_1 = 0$, the coefficient of y^{t-2} would be $\frac{e(e-1)}{2}\phi^2 + \sigma_2$. Since e=2m where m is odd, $\frac{e(e-1)}{2} = 1$ so that setting $\phi^2 = \sigma_2$ would make the whole coefficient of y^{t-2} zero.

3.24 Comments on the transformations

When some of the σ_i's are zero, $|\rho(y)|$ can be greater than, or

equal to, $|\sigma(x)|$. For instance, if $\sigma(x) = x^3 + \sigma_2 x + \sigma_3$, then $\rho(y)$ $= y^3 + y^2\phi + (\phi^2 + \sigma_2)\, y + \sigma_2\phi + \sigma_3$, where $x = y + \phi$. Here we see that at best we can make $|\rho(y)| = |\sigma(x)|$ by setting $\phi = \sqrt{\sigma_2}$. In such a situation we do not gain anything by the transformation. Thus the only definite comment we can make is as follows:

The transformation is advantageous when no σ_i is zero in 3.21 and 3.22, and only $\sigma_1 = 0$ in 3.23.

3.25 Examples

(i) If e = 3, then

$$\rho(y) = (y+\sigma_1)^3 + \sigma_1(y+\sigma_1)^2 + \sigma_2(y+\sigma_1) + \sigma_3$$
$$= y^3 + \sigma_2 y + \sigma_1\sigma_2 + \sigma_3.$$

(ii) If e = 4, then

$$\rho(y) = (y+\frac{\sigma_2}{\sigma_1})^4 + \sigma_1(y+\frac{\sigma_2}{\sigma_1})^3 + \sigma_2(y+\frac{\sigma_2}{\sigma_1})^2$$
$$+\sigma_3(y+\frac{\sigma_2}{\sigma_1}) + \sigma_4$$
$$= y^4 + (\frac{\sigma_2}{\sigma_1})^4 + \sigma_1(y^3 + \frac{\sigma_2}{\sigma_1}y^2 + \frac{1}{\sigma_1^2}\sigma_2^2 y + \frac{\sigma_2^3}{\sigma_1^3}) +$$
$$\sigma_2(y^2 + \frac{\sigma_2^2}{\sigma_1^2}) + \sigma_3(y + \frac{\sigma_2}{\sigma_1}) + \sigma_4.$$

or,

$$y^4 + y^3(\sigma_1) + y^2(\sigma_2 + \sigma_2) + y\left(\frac{\sigma_2^2}{\sigma_1} + \sigma_3\right) + \left(\frac{\sigma_2}{\sigma_1}\right)^4 + \frac{\sigma_2^3}{\sigma_1^2} + \frac{\sigma_2\sigma_3}{\sigma_1} + \sigma_4$$

$$= y^4 + \sigma_1 y^3 + \left(\frac{\sigma_2^2}{\sigma_1} + \sigma_3\right)y + \frac{\sigma_2^4}{\sigma_1^4} + \frac{\sigma_2\sigma_3}{\sigma_1} + \sigma_4.$$

(iii) If $e = 6$ and $\sigma_1 = 0$, then

$$\rho(y) = (y + \sqrt{\sigma_2})^6 + \sigma_2(y + \sqrt{\sigma_2})^4 + \sigma_3(y + \sqrt{\sigma_2})^3 + \sigma_4(y + \sqrt{\sigma_2})^2 + \sigma_5(y + \sqrt{\sigma_2}) + \sigma_6$$

$$= y^6 + y^4(\sqrt{\sigma_2})^2 + y^2(\sqrt{\sigma_2})^4 + (\sqrt{\sigma_2})^6 + \sigma_2(y^4 + \sigma_2^2) + \sigma_3(y^3 + y^2\sqrt{\sigma_2} + y\sigma_2 + (\sqrt{\sigma_2})^3 + \sigma_4(y^2 + \sigma_2) + \sigma_5(y + \sqrt{\sigma_2}) + \sigma_6$$

$$= y^6 + y^4(\sigma_2 + \sigma_2) + y^3(\sigma_3) + y^2(\sigma_2^2 + \sigma_3\sqrt{\sigma_2} + \sigma_4) + y(\sigma_3 + \sigma_2 + \sigma_5) + \sigma_2^3 + \sigma_2^3 + \sigma_3(\sqrt{\sigma_2})^3 + \sigma_4\sigma_2 + \sigma_5\sqrt{\sigma_2} + \sigma_6$$

or

$$\rho(y) = y^6 + \sigma_3 y^3 + y^2(\sigma_2^2 + \sigma_3\sqrt{\sigma_2} + \sigma_4) + y(\sigma_3\sigma_2 + \sigma_5) + \sigma_3(\sqrt{\sigma_2})^3 + \sigma_4\sigma_2 + \sigma_5\sqrt{\sigma_2} + \sigma_6.$$

3.26 Analysis of $\sigma(x)$ for the case of $t = 2$

when $t = 2$, we have

$$\sigma(x) = x^2 + \sigma_1 x + \sigma_2.$$

To find the roots of $\sigma(x)$, let us set

$$x^2 + \sigma_1 x + \sigma_2 = 0 \qquad (3\text{-}7)$$

or

$$\frac{x}{\sqrt{\sigma_2}} + \frac{\sigma_1}{\sqrt{\sigma_2}} + x^{-1}\sqrt{\sigma_2} = 0.$$

Setting $\frac{x}{\sqrt{\sigma_2}} = Z$ and $\frac{\sigma_1}{\sqrt{\sigma_2}} = \psi$, we have

$$Z + \psi + Z^{-1} = 0,$$

or

$$Z + Z^{-1} = \psi. \qquad (3\text{-}8)$$

Suppose $Z = \alpha^{a_1}$ and $Z = \alpha^{a_2}$ both satisfy this relation. Then we have

$$\alpha^{a_1} + \alpha^{-a_1} = \alpha^{a_2} + \alpha^{-a_2},$$

or

$$\alpha^{a_1} + \alpha^{a_2} = \alpha^{-a_1} + \alpha^{-a_2} = \frac{\alpha^{a_1+a_2}}{\alpha^{a_1+a_2}},$$

or

$$\alpha^{a_1+a_2} = 1.$$

This means that $a_1 = a_2$ or $a_1 = n - a_2$.

Thus for a given ψ, (3-8) has two unique solutions α^{γ} and $\alpha^{n-\gamma}$ where, without losing any generality, we can take $\gamma \leq \frac{n-1}{2}$. Hence γ can be found in at most $\frac{n-1}{2}$ trials. Once we have γ, the two roots of $\sigma(x)$ are given

$$x = \alpha^{\gamma}\sqrt{\sigma_2} \text{ and } x = \alpha^{n-\gamma}\sqrt{\sigma_2}.$$

on the other hand getting the roots of $\sigma(x)$ directly can take

at most n-1 trials. Therefore solving (3-8) takes less time on the average. It is also possible that we can store the sum $\alpha^{\gamma} + \alpha^{n-\gamma}$, for $\gamma = 1, 2, \ldots, \frac{n-1}{2}$, and use it as a look-up table.

For EXAMPLE suppose $E(x) = x^{12}(1+x^2)$ with repect to (15, 7, 2) BCH code with $g(x) = (1+x+x^4)(1+x+x^2+x^3+x^4)$. Then, using the $GF(2^4)$ given in Chapter 1, we have

$$S_1 = \alpha^{12} + \alpha^{14} = \alpha^5,$$

$$S_3 = \alpha^6 + \alpha^{12} = \alpha^4,$$

so that

$$\sigma_1 = S_1 = \alpha^5,$$

$$\sigma_2 = \frac{S_1^3 + S_3}{S_1} = \frac{1+\alpha^4}{\alpha^5} = \frac{\alpha}{\alpha^5} = \alpha^{11}.$$

Therefore

$$\sigma(x) = x^2 + \alpha^5 x + \alpha^{11}.$$

Clearly it takes 12 trials before we get the first root.

On the other hand

$$\psi = \frac{\sigma_1}{\sqrt{\sigma_2}} = \frac{\alpha^5}{\alpha^{13}} = \alpha^{-8} = \alpha^7,$$

so that

$$Z + Z^{-1} = \alpha^7.$$

Setting $Z = \alpha^j$, we have

$$\alpha + \alpha^{14} = 1 + \alpha + \alpha^3 = \alpha^7 .$$

Therefore, the roots of $Z + Z^{-1} = \alpha^7$ are α^1 and α^{15-1}. Hence the roots of $\sigma(x)$ are

$$x = \alpha^1 \sigma_2 = \alpha^1 \alpha^{13} = \alpha^{14},$$
$$x = \alpha^{14} \sigma_2 = \alpha^{14} \alpha^{13} = \alpha^{12}.$$

Consequently $E(x) = x^{12} + x^{14}$.

The look-up table for $Z + Z^{-1} = \psi$ over the $GF(2^4)$ generated by $1 + x + x^4$ is as follows :

$$\alpha^1 + \alpha^{14} = \alpha^1 + 1 + \alpha^3 = \alpha^7,$$
$$\alpha^2 + \alpha^{13} = \alpha^2 + 1 + \alpha^2 + \alpha^3 = \alpha^{14},$$
$$\alpha^3 + \alpha^{12} = \alpha^3 + 1 + \alpha + \alpha^2 + \alpha^3 = \alpha^{10},$$
$$\alpha^4 + \alpha^{11} = 1 + \alpha + \alpha + \alpha^2 + \alpha^3 = \alpha^{13},$$
$$\alpha^5 + \alpha^{10} = \alpha + \alpha^2 + 1 + \alpha + \alpha^2 = 1,$$
$$\alpha^6 + \alpha^9 = \alpha^2 + \alpha^3 + \alpha + \alpha^3 = \alpha^5,$$
$$\alpha^7 + \alpha^8 = 1 + \alpha + \alpha^3 + 1 + \alpha^2 = \alpha^{11}.$$

There are $\frac{15-1}{2} = 7$ distinct sums. Using the look-up table we get $\alpha^1 + \alpha^{14} = \alpha^7$. Therefore this is another way of getting the roots of $Z + Z^{-1} = \psi$.

CONCLUDING REMARKS

In the thesis we have dealt with the problem of decoding binary BCH codes. From the discussion in Chapter 3 it is seen that the task of getting the error locator polynomial is relatively simple when the expressions, like the ones shown in , say , 3-13, for elememtary functions are stored. The storing of these expressions is quite practical for small values of t. When t is large , a scheme like Berlekamp algorithm is more efficient.

The transformations discussed in 3.20-3.23 should prove useful, when used under appropriate conditions, in reducing the amount of computation involved in finding the roots of the error locator polynomial.

As pointed out in 3.18 , codes with even minimun distance are slightly better than the regular BCH codes in the sense of decoding.

It was also seen in 3.26 that finding the roots of the quadratic became comparitively simple after defining a new varible. It may prove useful to investigate whether this type of thinking can be extended to polynomials of even degree greater than two.

REFERENCES

W.W. Peterson and E.J. Weldon Jr; "Error-Correcting Codes " Second Edition, MIT Press, pp. 1-16, pp. 269-308, Chap 1 and Chap 9. 1972.

Shu Lin ; " An Introduction to Error-Correcting Codes " Prentice-Hall Inc; New Jersey pp. 112-139, pp. 185-211, Chap 6, Chap 8 and Chap 9. 1970.

J.L. Massey; " Threshold Decoding ", MIT Press Research Monograph 20, Cambridge, Mass; The MIT Press.

R.C. Bose and D.K. Ray-Chaudhuri; " Further Results on Error Correcting Binary Group Codes ", Inf and Control. 3, pp. 279-290, 1969.

W.W. Peterson; " Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes ", IEEE Trans. on Inf. Theo; Vol 6, pp. 459-470, 1960.

C. V. Srinivasan; " Codes for Error Correction in High-Speed Memory Systems—Part I : Correction of Cell Defects in Integrated Memories", IEEE Trans. Computers. Vol. C-20. pp. 882-888, 1971, and

———————; " Codes for Error Correction in High-Speed Memory Systems —Part II : Correction of Temporary and Catastrophic Errors ", IEEE Trans. Computers. Vol. C-20. pp. 1514-1520, 1971.

A. Hocquenghem; " Codes Correcteurs d'Erreurs ", Chiffres, 2, pp. 147-156, 1959.

E.R. Berlekamp; " Algebraic Coding Theory ", Mcgraw-Hill Book Company, N.Y, 1968. pp. 176-199, Chap 7.

9. J.L. Massey; " Shift - Register Synthesis and BCH Decoding",
IEEE Trans. on Inf. Theo; IT-15, pp. 122-127, 1969.

10. R.T. Chien; " Cyclic Decoding Procedure for Bose-Chaudhuri-
Hocqenghem Codes " IEEE Trans. Inf. Theo; Vol. IT-10,
pp. 357-363, 1964.

11. H.O. Burton; " Inversionless Decoding of Binary BCH Codes",
IEEE Trans. on Inf. Theo; Vol. IT-17, pp. 464-466, 1971.

12. Birkhoff, G; and S. Maclane, " A Survey of Modern Algebra ",
MacMillan, NY. pp. 33-82. 1941.

VITAE

Full Name :	Hsiu Lu Chao.
Birth Place :	Haulien, Taiwan.
Birth Date :	Febuary 2, 1947.
High School :	National Normal University Attached High School. Taipei, Taiwan.
Baccalaureate :	Tatung Institute of Technology, Taipei, Taiwan.