SOME ASPECTS OF BINARY CYCLIC CODES

by

Rémy Roy

Submitted in partial fulfilment of the requirements for the degree of Master of Science.

Department of Electrical Engineering,
Faculty of Pure and Applied Science,
The University of Ottawa,
Ottawa, CANADA.

August, 1968.

ABSTRACT

Let us consider the relation $1 + X^n = g(X)\ h(X)$ where $g(X)$ and $h(X)$ are polynomials over GF(2) (with coefficients from the Galois Field of two elements) and $n = 2^q - 1$, q a positive integer. It is well known that for a code of length n generated by $g(X)$, $h(X)$ can act as a parity check when appropriately used. In this context, the present thesis takes an approach based on the consideration of each $g_i(X)$ and $h_i(X) = (1 + X^n)/g_i(X)$, $g_i(X)$ being a factor of $g(X)$, rather than $g(X)$ and $h(X)$ themselves.

This approach brings out certain interesting possibilities though it does not produce any startlingly new results. Specifically, the approach will be used, by way of illustration, to analyse Abramson codes and the case of $1 + X^{31}$

ACKNOWLEDGEMENTS

The author wishes to take this opportunity to extend his sincere gratitude to Professor S. G. S. Shiva for suggesting the topic of this thesis and guidance in the course of the development of the thesis.

The author would like to thank his colleagues P. E. Allard, T. Zeitoun and G. Seguin for their helpful suggestions.

Finally, the author is greatful to the National Research Council of Canada and the University of Ottawa for their financial assistance.

TABLE OF CONTENTS

1. INTRODUCTION

In an ideal system the binary symbol that comes out of the channel-to-binary decoder should match the symbol that entered the binary-to-channel encoder. In a practical system (Figure 1) there are occasional errors and it is the purpose of binary codes to detect and perhaps correct such errors.

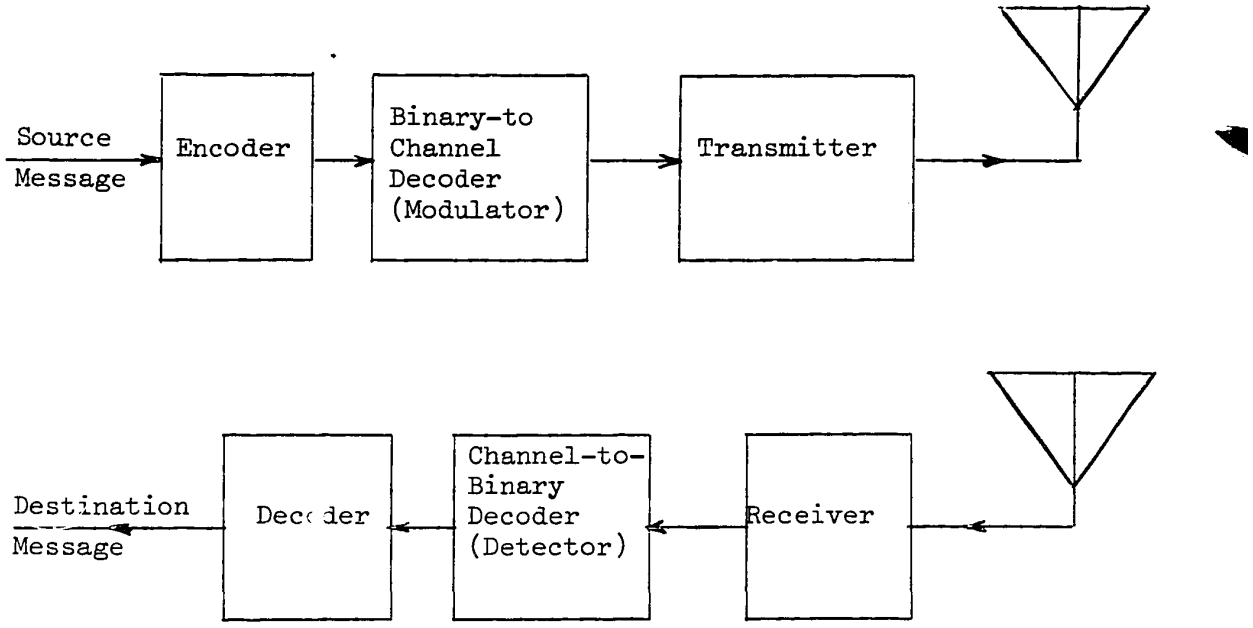

Figure 1. Block diagram of a communication system

These codes cannot correct every conceivable pattern of errors but rather must be designed to correct the most likely patterns of errors.

The design and construction [1] of codes is based on the assumption that each bit in a binary sequence is affected independently by noise. But quite frequently [2], in some systems, errors do not occur independently but rather in bursts; telephone lines and magnetic storage are examples of such systems. Telephone-line disturbances, such as lightning, last longer than the time for one symbol. Magnetic-tape defects are larger than the space required for a symbol. Consequently, codes for correcting bursts of errors are required, and some remarkably good codes such as Fire codes and Abramson codes, to name a few, have been developed for this purpose.

Coding is the process by which the information to be transmitted is rearranged or changed into some other format suitable for transmission.

In this context the purpose of this thesis is to describe an approach by means of which the burst error correcting capability of a given binary cyclic code can be found with relative ease.

The material to follow is organized into 4 main chapters. Chapter 2 defines some important algebraic structures. Chapter 3 gives a description of some well known codes. Chapter 4 derives an approach to find the burst error correcting capability of a given binary cyclic code. The main points of chapter 4 have been covered in a technical report [3]. Chapter 5 gives some concluding remarks.

2. SOME ALGEBRAIC CONCEPTS

Algebraic structures have been the basis of all of the known important codes. This chapter defines those algebraic structures which are important and pertinent to this thesis. Also relevant theorems are given without proof. The proofs themselves may be found in any Algebra text book [4,5].

2.1. Groups

A set G is called a **group**, with respect to one operation, multiplicative or additive, if the following axioms are satisfied:

1. For any two elements a,b of G
   a * b is also in G (closure).
2. For any three elements a,b,c of G
   a * (b * c) = (a * b) * c (associative law).
3. Among the elements of G there exist an
   element I such that for every a of G
   a * I = I * a = a (identity).
4. For every element a of G there exist an
   element a^{-1} of G such that
   $a * a^{-1} = a^{-1} * a = I$ (inverse).

In addition to the above axioms a group may satisfy the commutative property, i.e., if, for any two elements a,b of G,

$$a * b = b * a,$$

then such a group is called **abelian** or **commutative.**

2.2. Rings

A set R, with respect to two operations, addition denoted by a + b and multiplication denoted by ab (these operations may not be ordinary addition and multiplication), is called a **ring** if the following axioms are satisfied:

1. The set R is an abelian group under addition,
2. For any two elements a,b of R, the product ab is defined and is an element of R (closure),
3. For any three elements a,b,c of R,
   $a(bc) = (ab)c$ (associative law)
4. For any three elements a,b,c of R,
   $a(b + c) = ab + ac$ and
   $(b + c)a = ba + ca$ (distributive law).

A ring is called commutative if its multiplication operation is commutative, i.e., for any two elements, a,b of R, $ab = ba$.

2.3. Fields

A **field** is a commutative ring with unit element (multiplicative identity) in which every nonzero element has a multiplicative inverse. Field elements are called **scalars**.

2.4. Subgroups

A subset of elements of a group G is called a **subgroup** H if it satisfies all the axioms of a group itself.

To determine if H is a subgroup it is only necessary to check for closure and for inverse properties. The set of n-tuples denoted $(a_1, a_2, \ldots a_n)$ where $a_i = 0$ or 1 forms a group with respect to modulo 2 addition. In this group every element is its own inverse. Therefore a subset is a subgroup if it contains the **zero** element (0,0,0,...,0) and if it is closed under addition.

Consider a group G whose elements are $g_1, g_2, g_3, \ldots$ and a subgroup H of elements $h_1, h_2, h_3, \ldots$ and the array (Figure 2.1) formed as follows: the first row is the subgroup, with the identity element at the left and each other element appearing once and only once. The first element in the second row is any element not appearing in the first row, and the rest of the elements are obtained by multiplying each subgroup element by this first element on the left. Similarly a third, fourth, fifth,etc... row are formed, each with a previously unused group element.

in the first column, until all the group elements have been exhausted.

$$
\begin{array}{llllll}
h_1 = 1, & h_2, & h_3, & \ldots, & h_n \\
g_1 h_1 = g_1, & g_1 h_2, & g_1 h_3, & \ldots, & g_1 h_n \\
g_2 h_1 = g_2, & g_2 h_2, & g_2 h_3, & \ldots, & g_2 h_n \\
\vdots & & & & \\
g_m h_1 = g_m, & g_m h_2, & g_m h_3, & \ldots, & g_m h_n
\end{array}
$$

Figure 2.1. Cosets of subgroup H

The set of elements in a row of this array is called a left coset, and the elements appearing in the first column is called the coset leader. Right cosets could be similarly formed. Whenever the group G is commutative, then for any subgroup H, aH = Ha for every element a of G, i.e., left coset = right coset. Since the group of n-tuples $(a_1, a_2, \ldots, a_n)$ $(a_i = 0 \text{ or } 1)$ forms a commutative group under modulo 2 addition then it follows that left cosets coincide with right cosets.

2.5. Vector Spaces and Linear Algebras

A set V is called a vector space over a field F if the following axioms are satisfied:

1. The set V is an abelian (commutative) group under addition,

2. For any vector v and any field element c, a product cv, which is a vector, is defined,
3. For any two vectors u and v of V and any field element c of F

$$c(u + v) = cu + cv \text{ (distributive law)},$$

4. For any vector v of V and any two field elements c, d of F

$$(cd)v = c(dv) \text{ and}$$

$$1v = v \text{ (associative law)}.$$

A set A is called a **linear associative algebra** over a field F if the following axioms are satisfied:

1. The set A is a vector space over F,
2. For any two elements u, v of A there is a product uv defined that is in A,
3. For any three elements u, v, w of A

$$(uv)w = u(vw) \text{ (associative law)},$$

4. For any two elements c, d of F and any three elements u, v, w of A

$$u(cv + dw) = cuv + duw \text{ and}$$

$$(cv + dw)u = cvu + dwu \text{ (bilinear law)}.$$

The set of all linear combinations of a set of vectors $v_1, v_2, \ldots, v_n$ of a vector space v is a subspace of V. The set of vectors $v_1, \ldots, v_n$ is linearly dependent if and only if there are scalars $c_1, \ldots c_n$, not all zero, such that $c_1 v_1 + c_2 v_2 + \ldots + c_n v_n = 0$.

A set of vectors is said to span a vector space if every vector in the vector space equals a linear combination of the vectors in the set In any space the number of linearly independent vectors that span the space is called the dimension of the space.

2.6. Subspaces

A subset of a vector space V is called a subspace S if all the axioms for a vector space are satisfied by the elements of S.

2.7. Null Spaces

A subspace S_1 is called the null space of another subspace S_2 if the set of vectors in S_1 are orthogonal to the set of vectors of S_2.

2.8. Ideals

An ideal I is a subset of elements of a ring R with the following two properties:

1. I is a subgroup of the additive group of R,
2. For any element a of I and any element r of R, ar and ra belong to I.

2.9. Residue classes

Let R be a ring under addition and multiplication $(R, +, \cdot)$ and $(S, +, \cdot)$ be an ideal. Since $(S, +)$ is a subgroup of $(R, +)$, we can form cosets, as described previously. In this case these cosets are referred to as residues or residue classes. We denote a residue class, with leader a, as $\{a\}$ where $\{a\} = a + S = \{a + s : s \in S\}$. We now define two operations between residues as:

$$\{a\} \oplus \{b\} = \{a + b\}$$

$$\{a\} * \{b\} = \{ab\}.$$

It can be shown that $(R/S, \oplus, *)$ forms a ring where R/S denotes the collection of residues modulo S, i.e., $R/S = \{r + S : r \in R\}$. This ring is referred to as the residue class ring. A case of interest is when R is the set of integers. Inthis case the set of all multiples of an integer m is an ideal and is denoted by (m) where

$$(m) = \{km : k \in R\}.$$

The residue class ring $(R/(m), \oplus, *)$ is called the ring of integers modulo m. The residue class ring modulo m is a field if and only if m is a prime number. These fields are called prime fields or Galois fields of p elements denoted by GF(p).

The remaining of this chapter is devoted to polynomial rings and Galois fields.

2.10. Polynomial Ideals and Residue classes

Now consider polynomials f(X), with one independent variable X and with coefficients from any field F:

$$f(X) = f_0 + f_1 X + f_2 X^2 + \ldots + f_n X^n, \quad f_i \in F.$$

The degree of a polynomial is the largest power of X in a term with nonzero coefficient. The degree of the 0 polynomial is 0. A polynomial is called monic if the coefficient of the highest power of X is 1.

If r(X), s(X), and t(X) are polynomials and r(X) s(X) = t(X), then it is said that t(X) is divisible by r(X) or that r(X) divides t(X), and that r(X) is a factor of t(X). A polynomial p(X) of degree n which is not divisible by any polynomials of degree less than n but greater than 0 is called irreducible. The greatest common divisor of two polynomials is the monic polynomial of greatest degree which divides both of them. Two polynomials are said to be relatively prime if their greatest common divisor is 1. A polynomial $f^*(X)$ is said to be the reciprocal of f(X) of degree r if the coefficients of X^{r-i} in $f^*(X)$ is the same as of X^i in f(X), for i = 0, 1, 2, . . . , r. If $f(X) = 1 + X + X^4$, then $f^*(X) = 1 + X^3 + X^4$, r = 4.

A set of polynomials is an ideal if and only if it consists of all multiples of some polynomial.

Every residue class modulo a polynomial f(X) of degree n contains either 0 or a polynomial of degree less than n. Zero is an element of the ideal, and every polynomial of degree less than n is in a distinct residue class.

The residue classes of polynomials modulo a polynomial f(X) of degree n form a commutative linear algebra of dimension n over the coefficient field.

2.11. Galois Fields

Let p(X) be a polynomial of degree k with coefficients in a field F. If p(X) is irreducible in F, i.e., if p(X) has no factor with coefficients in F, then the algebra of polynomials over F modulo p(X) is a field. The field thus formed is called an extension field of degree k over F. If the residue classes containing X is called α, the extension field is denoted $F[\alpha]$. The original field F is called the ground field. The new field contains an element (a residue class) corresponding to each element in the ground field, and it is said that it contains the ground field. Since $p(\alpha) = 0$, α is a root of p(X), and it is said that the extension field is obtained by adjoining a root of p(X) to F.

Now consider a ground field F and an extension field, and let β be an element of the extension field. The monic polynomial m(X) of smallest degree with coefficients in the ground field F, such that $m(\beta) = 0$, is called the minimum polynomial or the minimum function of β.

Then it can be shown [5] that the minimum function $m(X)$ of any element β is irreducible.

2.12. The Multiplicative Group of a Galois Field

Consider in any finite group the set of elements formed by any element α and all its powers $\alpha\alpha = \alpha^2$, $\alpha\alpha^2 = \alpha^3$, and so on. There can be at most a finite set of such elements and therefore at some point there must be repetition, i.e., $\alpha^i = \alpha^j$ for some i and j. Then multiplying by $(\alpha^i)^{-1} = (\alpha^{-1})^i$ gives $1 = \alpha^{j-i}$. Therefore α to some power equals 1. Let e be the smallest positive integer such that $\alpha^e = 1$. Then e is called the order of the element α. Then the set $1, \alpha, \alpha^2, \ldots, \alpha^{e-1}$ forms a multiplicative subgroup. A group that consist of all the powers of one of its elements is called a cyclic group.

In GF(q), there is a primitive element α, i.e., an element of order $q - 1$, such that every nonzero element can be expressed as a power of α, i.e., the multiplicative cyclic group GF(q).

Example:

The Galois field of 2^4 elements $GF(2^4)$ may be formed as a field of polynomials over GF(2) modulo $1 + X + X^4$. Let α denote the residue class containing X. Then α is a root of $1 + X + X^4$, and it happens to be a primitive element of the field. Then the 15 nonzero elements are given in Table 2.1.

Table 2.1. Field Elements Representation of $GF(2^4)$ Generarated by $1 + X + X^4$

$$\alpha^0 = 1 = (1\ 0\ 0\ 0)$$
$$\alpha^1 = \alpha = (0\ 1\ 0\ 0)$$
$$\alpha^2 = \alpha^2 = (0\ 0\ 1\ 0)$$
$$\alpha^3 = \alpha^3 = (0\ 0\ 0\ 1)$$
$$\alpha^4 = 1 + \alpha = (1\ 1\ 0\ 0)$$
$$\alpha^5 = \alpha + \alpha^2 = (0\ 1\ 1\ 0)$$
$$\alpha^6 = \alpha^2 + \alpha^3 = (0\ 0\ 1\ 1)$$
$$\alpha^7 = 1 + \alpha + \alpha^3 = (1\ 1\ 0\ 1)$$
$$\alpha^8 = 1 + \alpha^2 = (1\ 0\ 1\ 0)$$
$$\alpha^9 = \alpha + \alpha^3 = (0\ 1\ 0\ 1)$$
$$\alpha^{10} = 1 + \alpha + \alpha^2 = (1\ 1\ 1\ 0)$$
$$\alpha^{11} = \alpha + \alpha^2 + \alpha^3 = (0\ 1\ 1\ 1)$$
$$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3 = (1\ 1\ 1\ 1)$$
$$\alpha^{13} = 1 + \alpha^2 + \alpha^3 = (1\ 0\ 1\ 1)$$
$$\alpha^{14} = 1 + \alpha^3 = (1\ 0\ 0\ 1)$$
$$\alpha^{15} = 1 = \alpha^0$$

3. THEORY OF BINARY CYCLIC CODES

3.1. Basis of Binary Cyclic Codes

Cyclic codes are based on the following theorem: let $f(X) = g(X)\ h(X)$ where $f(X)$ has degree n and $h(X)$ has degree k. Then the ideal generated by $g(X)$ in the algebra of polynomial modulo $f(X)$ has dimension k [6].

The monic polynomial $g(X)$ of minimum degree such that $\{g(X)\}$ is in an ideal I is called the generator of the ideal. Every ideal in the algebra of polynomial modulo $f(X)$ has a generator polynomial $g(X)$ that divides $f(X)$, and conversely every monic polynomial that divides $f(X)$ generates a different ideal. Every residue class in the ideal generated by $g(X)$ contains a unique polynomial that is divisible by $g(X)$ and has degree less than that of $f(X)$. Every such polynomial is in a residue class that is in the ideal.

Consider the polynomial $f(X) = X^n + 1$, belonging to the ring of polynomial with coefficients from GF(2), being represented as the product of two polynomials

$$X^n + 1 = g(X)\ h(X)$$

where $h(X)$ has degree k and $g(X)$ has degree $n - k$. Figure 3.1 represents

all the residue classes of the ideal generated by $X^n + 1$ (this is the same as forming the cosets of a subgroup).

$$
\begin{aligned}
\{0\} &= 0(X^n+1) && X^0(X^n+1) && X(X^n+1) \ldots \\
\{g_1(X)\} &= g_1(X) + 0(X^n+1) && g_1(X) + X^0(X^n+1) && g_1(X) + X(X^n+1) \ldots \\
\{g_2(X)\} &= g_2(X) + 0(X^n+1) && g_2(X) + X^0(X^n+1) && g_2(X) + X(X^n+1) \ldots \\
&\vdots \\
\{g_{2^n-1}(X)\} &= g_{2^n-1}(X) + 0(X^n+1) && g_{2^n-1}(X) + X^0(X^n+1) && g_{2^n-1}(X) + X(X^n+1) \ldots
\end{aligned}
$$

Figure 3.1. Residue classes of the ideal generated by $X^n + 1$

The above array contains all the polynomials in the ring of polynomials with coefficients 0 and 1, i.e., each row in the array is a residue class which cannot contain more than one polynomial of degree less than n. In other words there are as many residue classes modulo $X^n + 1$ as there are polynomials of degree less than n and that is 2^n.

Referring to the polynomial $X^n + 1 = g(X)\, h(X)$, it would be found that somewhere amongst all the residue classes $\{0\}$, $\{g_1(X)\}$, $\{g_2(X)\}$, . . . , $\{g_{2^n-1}(X)\}$, there exists a residue class containing the polynomial $g(X)$ which naturally divides $X^n + 1$. Since $g(X)$ and $h(X)$ have

degrees n-k and k respectively then the ideal generated by g(X) is a vector subspace of dimension k with basis vectors $\{g(X)\}$, $\{X\ g(X)\}$, $\{X^2 g(X)\}$, . . . , $\{X^{k-1} g(X)\}$.

A subspace V of n-tuples is called a cyclic subspace or a cyclic code if for each vector $v = (a_0, a_1, a_2, \ldots, a_{n-1})$ in V, the vector $v' = (a_{n-1}, a_0, a_1, a_2, \ldots, a_{n-2})$ obtained by shifting the conponents of v cyclically one unit to the right, is also in V.

It has been shown [7] that in the ring of polynomials modulo $X^n + 1$, a subspace is a cyclic code if and only if it is an ideal. Hence a cyclic code is completely specified by a polynomial g(X) that divides $X^n + 1$, or by the null space of the ideal generated by $h(X) = (X^n + 1)/g(X)$. For g(X) of degree n - k and h(X) of degree k, the code has dimension k. The element $\{f(X)\}$ is in the code if and only if f(X) is divisible by g(X). This code will be referred to as an (n, k) cyclic code.

In matrix representation

$$G = \begin{bmatrix} g(X) \\ X\ g(X) \\ X^2\ g(X) \\ \vdots \\ X^{k-2}\ g(X) \\ X^{k-1}\ g(X) \end{bmatrix}.$$

If $g(X) = g_0 + g_1 X + g_2 X^2 + \ldots + g_{n-k} X^{n-k}$ then

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 & \cdots & 0 \\ \cdot & & & & & & & & \\ \cdot & & & & & & & & \\ \cdot & & & & & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_{n-k} & \end{bmatrix}.$$

All the rows of G are code vectors, they are linearly independent and the rank of G is k which is also the dimension of the code. All linear combination of the rows of G forms the entire code, i.e., the row space of G is the code space. However, the theorem does not give the error correcting capability. All it says is that $\{g(X)\}$ and its k - 1 right cyclic shifts are linearly independent and that their linear combination gives a binary cyclic code.

Now, since polynomial multiplication and dot or inner product of vectors differ, we form the matrix H^* by taking $\{h^*(X)\}$, $\{X^{-1} h^*(X)\}$, $\{X^{-2} h^*(X)\}$, ..., $\{X^{-n+k+1} h(X)\}$ where $h^*(X)$ is the reciprocal polynomial of $h(X)$ with respect to n - 1. If

$$h(X) = h_0 + h_1 X + h_2 X^2 + \ldots + h_k X^k$$

then

$$h^*(X) = h_k X^{n-1-k} + h_{k-1} X^{n-k} + \ldots + h_2 X^{n-3} + h_1 X^{n-2} + h_0 X^{n-1}$$

and

$$H^* = \begin{bmatrix} 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_2 & h_1 & h_0 \\ 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 \\ \cdot & & & & & & & & & \\ \cdot & & & & & & & & & \\ \cdot & & & & & & & & & \\ 0 & h_k & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & \cdots & 0 \\ h_k & h_{k-1} & \cdots & h_2 & h_1 & h_0 & 0 & \cdots & 0 \end{bmatrix}.$$

In other words, H^* consists of $h^*(X)$ and its $n - k - 1$ left cyclic shifts. Then it can easily be verified that $G(H^*)^T = 0$. Then H^* can act as a parity check matrix when appropriately used. This code is equivalent to the Hamming (n, k) code since the columns of H^* will all be distinct. For any received vector $R = \{r(X)\}$, the $n - k$ component vector S, $S = R(H^*)^T$, has been called variously by the names of syndrome , parity check, and corrector.

3.2. Bose-Chaudhuri-Hocquenghem Codes

Bose and Ray-Chaudhuri [8, 9], and at about the same time, Hocquenghem [10] have developed a class of binary codes of lenght $n = 2^m - 1$ for an arbitrary positive integer m. These codes can correct t random errors and require no more than mt parity check digits. Thus the BCH (Bose-Chaudhuri-Hocquenghem) (n, k, t) codes, Where k is the number of information digits, cover a wide range of transmission rate, $R = k/n$, and error correcting capability. These codes are a remarkable generalization

of Hamming codes [11]. The BCH codes are cyclic codes and are best defined in terms of the roots of the generator polynomial. What Bose-Chaudhuri-Hocquenghem did was to give a formula to construct the generator polynomial g(X) to have a required error correcting capability.

3.2.1. Encoding Procedure

Given an irreducible polynomial p(X) of degree m with coefficients 0 and 1, a representation of the Galois field with 2^m elements $GF(2^m)$ can be formed. It consists of all polynomials of degree m - 1 or less. They can be added (modulo 2) term by term in the ordinary way. There is no special rule for multiplication except that the answer is reduced modulo 2 and modulo p(X) to a polynomial of degree m - 1 or less. It can be shown that certain polynomials p(X) have for their roots primitive elements, and will therefore generate the multiplicative cyclic group (all nonzero elements) of the $GF(2^m)$ as shown in section 2.12 of this thesis.

Definition and encoding procedures for the BCH codes have been covered in detail in [8]. An alternative and more general definition [9, 12] shows that BCH codes are examples of cyclic codes.

By the alternative definition of BCH codes, a generator polynomial g(X) is one which has for its roots α, α^3, α^5, . . ., α^{2t-1}.

Each element α^j of the field is a root of a unique irreducible polynomial $m_j(X)$ of minimum degree. Then g(X) must be divisible by $m_1(X)$,

$m_3(X)$, $m_5(X)$, . . ., $m_{2t-1}(X)$ and, hence, by their least common multiple:

$$g(X) = \text{LCM}\,[m_1(X), m_3(X), m_5(X), \ldots, m_{2t-1}(X)].$$

Since each of the factors of $m_j(X)$ is irreducible and has degree no greather than m, the least common multiple of g(X) is simply the product of the polynomials $m_j(X)$ with the duplicates omitted. Duplications are possible and will occur for any α^i and α^j that are roots of the same minimum function $m_i(X)$. Then for a given t and m, g(X) will generate a BCH binary code of length $n = 2^m - 1$ that will correct t-random errors or less and has no more than tm parity check digits.

Example:

For $m = 4$, $t = 3$ then $\{v(X)\}$ is a code word if and only if α, α^3, α^5 are roots of v(X), where α is a primitive element of $GF(2^4)$, then $\alpha^{15} = 1$, and the length of each code word is $n = 2^4 - 1 = 15$. Then the generator polynomial is given by

$$g(X) = m_1(X)\, m_3(X)\, m_5(X).$$

If $m_1(X)$ is the minimum function of α and is taken to be

$$m_1(X) = 1 + X + X^4$$

then α, α^2, α^4, α^8 are roots of $m_1(X)$, and $m_1(X) = m_2(X) = m_4(X) = m_8(X)$. Similarly, α^3, α^6, α^{12}, $\alpha^{24} = \alpha^9$ are roots of $m_3(X)$. This can be abbreviated by listing only the exponents.

1	2	4	8	$m_1(X) = m_2(X) = m_4(X)$ degree 4
3	6	12	9	$m_3(X) = m_6(X)$ degree 4
5	10			$m_5(X)$ degree 2

Then

$$g(X) = (1 + X + X^4)\ (1 + X + X^2 + X^3 + X^4)\ (1 + X + X^2)$$
$$= 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}$$

and

$$h(X) = (1 + X^{15}) \ / \ g(X) = 1 + X + X^3 + X^5.$$

This is BCH (15, 5) 3 errors or less correcting code.

3.2.2 Decoding Procedure

Relatively simple error correcting methods have been devised [13] for the t-error correcting BCH codes. If r(X) is the received polynomial, then r(X) can be expressed as a code word v(X) plus an error polynomial e(X):

$$r(X) = v(X) + e(X)$$

where $e(X) = \sum_{i=0}^{n-1} e_i X^i$, $e_i = 0$ or 1. The correction procedure consists of three phases:

1. Calculation of the parity checks and the even-numbered S_j, i.e.,

$$S_1 = r(\alpha), \quad S_3 = r(\alpha^3), \quad \ldots, \quad S_{2t-1} = r(\alpha^{2t-1})$$

and

$$S_2 = S_1^2, \quad S_4 = S_2^2, \quad \ldots, \quad S_{2t-2} = S_{t-1}^2.$$

Or equivalently $S_i = r(\alpha^i)$, $i = 1, 2, 3, \ldots, 2t$.

2. From the power sum symmetric functions S_i, we calculate the elementary symmetric functions σ_i

$$[A] \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \sigma_3 \\ \\ \\ \\ \sigma_{t-1} \\ \sigma_t \end{bmatrix} = \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ \cdot \\ \cdot \\ \cdot \\ S_{2t-3} \\ S_{2t-1} \end{bmatrix} \qquad (3.1)$$

where A is the matrix

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 \\ S_2 & S_1 & 1 & 0 & \cdots & 0 & 0 \\ S_4 & S_3 & S_2 & S_1 & \cdots & 0 & 0 \\ \cdot & & & & & & \\ \cdot & & & & & & \\ \cdot & & & & & & \\ S_{2t-4} & S_{2t-5} & S_{2t-6} & S_{2t-7} & \cdots & S_{t-4} & S_{t-3} \\ S_{2t-2} & S_{2t-3} & S_{2t-4} & S_{2t-5} & \cdots & S_{t-2} & S_{t-1} \end{bmatrix}. \qquad (3.2)$$

If the determinant of A is not equal to 0 ($|A| \neq 0$) then $t - 1$ or t errors have occurred and we solve (3.1) obtaining the values of $\sigma_1, \sigma_2, \ldots, \sigma_t$. If $|A| = 0$ then $t - 3$ or $t - 2$ errors have occrrred and matrix A is reduced to a $(t - 2)\times(t - 2)$ matrix by deleting the last row and column of A and we solve (3.1) to obtain $\sigma_1, \sigma_2, \ldots, \sigma_{t-2}$, etc...

3. Finally, substituting each field element, generated by $m_1(X)$, into the equation

$$X^t + \sigma_1 X^{t-1} + \sigma_2 X^{t-2} + \ldots + \sigma_{t-1} X + \sigma_t = 0,$$

then those field elements that satisfy this equation correspond to error location.

As a numerical example, consider the code of the previous example, i.e., $g(X) = 1 + X + X^2 + X^4 + X^5 + X^8 + X^{10}$. The field representation of $GF(2^4)$ generated by $m_1(X) = 1 + X + X^4$ are given in Table 2.1. Suppose that the vector $\{v(X)\} = \{g(X)\}$ is transmitted, and that errors occur in the third, sixth and eleventh position. Then the received polynomial is $r(X) = 1 + X + X^4 + X^8$. The power sum symmetric functions S_i are

$$\begin{aligned} S_1 &= r(\alpha) = \alpha^8 = (1\ 0\ 1\ 0), \\ S_2 &= S_1^2 = \alpha^1 = (0\ 1\ 0\ 0), \\ S_3 &= r(\alpha^3) = \alpha^6 = (0\ 0\ 1\ 1), \\ S_4 &= S_2^2 = \alpha^2 = (0\ 0\ 1\ 0) \text{ and} \\ S_5 &= r(\alpha^5) = \alpha^5 = (0\ 1\ 1\ 0). \end{aligned}$$

Substituting S_i in (3.2) we get

$$\left.\begin{aligned} \sigma_1 &= \alpha^8 \\ \alpha^1 \sigma_1 + \alpha^8 \sigma_2 + \sigma_3 &= \alpha^6 \\ \alpha^2 \sigma_1 + \alpha^6 \sigma_2 + \alpha^1 \sigma_3 &= \alpha^5 \end{aligned}\right\}. \tag{3.3}$$

Solving (3.3) for σ_i we get $\sigma_1 = \alpha^8$, $\sigma_2 = \alpha^8$ and $\sigma_3 = \alpha^2$. Then it can easily be verified that

$$X^3 + \alpha^8 X^2 + \alpha^8 X + \alpha^2 = 0$$

is satisfied by $X = \alpha^2$, α^5, α^{10}, and only these. The powers of α plus 1 are the error position number locations in the received sequence $\{r(X)\}$.

3.3. Abramson Codes

Abramson [14] has described a class of codes which corrects all bursts of length 2 or less, and another class [15] which corrects all bursts of length 3 or less.

3.3.1. Codes for Correcting Bursts of Length 2 or Less

The generator polynomial of a code that corrects bursts of length 2 or less, i.e., single errors (SE) and double adjacent errors (DAE), has the form

$$g(X) = p(X)\ (1 + X)$$

where $p(X)$ is a primitive polynomial of degree m. The length of the code $n \leq k + m + 1$, where k is the number of information digits. The factor $(1 + X)$ adds an extra parity check on all digits so that the code has $m + 1$ parity check digits. Then $(1 + X)$ specifies whether a SE or a DAE has occurred while $p(X)$ determines the actual error position.

3.3.2. Codes for Correcting Bursts of Length 3 or Less

Abramson also attempted to find minimum-redundancy binary cyclic codes for bursts of length 3 or less. It appears very likely that there exist primitive polynomials $p(X)$ of even degree, greater than 2, for

which the generator polynomial for a code that corrects all bursts of length 3 or less is given by

$$g(X) = p(X)\ (1 + X + X^2).$$

The generator polynomial $p(X)$ must be an irreducible polynomial of even degree m and a factor of $1 + X^n$ where $n = 2^m - 1$. But $(1 + X + X^2)$ must also be a factor of $1 + X^n$. The factor $(1 + X + X^2)$ will divide $1 + X^n$ if n is divisible by 3. Then $1 + X + X^2$ will also be a factor of $1 + X^3$.

We will show that, for an arbitrary even integer m, $n = 2^m - 1$ is divisible by 3. Let us assume that $n = 2^m - 1$ is divisible by 3. The question now, is $n = 2^{m+2} - 1$ divisible by 3 ?

$$2^{m+2} - 1 = (2^m)\ 2^2 - 1 \qquad (3.4)$$

To the term 2^m in (3.4), add and subtract 1, then

$$\begin{aligned} 2^{m+2} - 1 &= (2^m - 1 + 1)\ 2^2 - 1, \\ &= (2^m - 1)\ 2^2 + 2^2 - 1, \\ &= (2^m - 1)4 + 3. \end{aligned} \qquad (3.5)$$

But we have assumed that $2^m - 1$ was divisible by 3. Therefore, form (3.5), 3 also divides $2^{m+2} - 1$.

We have shown, by induction, that given an arbitrary even integer m, 3 divides $n = 2^m - 1$. This showed indirectly that $1 + X + X^2$ is a factor of $1 + X^n$ provided n satisfies the above conditions.

Then $g(X) = p(X)\ (1 + X + X^2)$ will generate a code that corrects bursts of length 3 or less if it satisfies the following conditions. First, if α is a root of p(X) then $\alpha^{n/3}$ is a root of $1 + X + X^2$. Secondly, the burst error pattern polynomials of degree 2 or less (bursts of length 3 or less) are $1,\ 1 + X,\ 1 + X^2,\ 1 + X + X^2$. The permissible error polynomials are $X^{a_1},\ X^{a_2}\ (1 + X),\ X^{a_3}\ (1 + X^2),\ X^{a_4}\ (1 + X + X^2)$ where $a_i + 1$ is the actual error position in a received sequence {r(X)}. Then

$$r(\alpha) = \alpha^{a_1},\ \alpha^{a_2}\ (1 + \alpha),\ \alpha^{a_3}\ (1 + \alpha^2),\ \alpha^{a_4}\ (1 + \alpha + \alpha^2), \qquad (3.6)$$

and

$$r(\alpha^{n/3}) = \alpha^{a_1 n/3},\ \alpha^{a_2 n/3}\ (1 + \alpha^{n/3}),\ \alpha^{a_3 n/3}\ (1 + \alpha^{2n/3}),\ 0, \qquad (3.7)$$

The last term of (3.7) is 0 since $\alpha^{n/3}$ is a root of $1 + X + X^2$. Through the multiplicative group of $GF(2^m)$ generated by p(X), we can express each of the term $1 + \alpha,\ 1 + \alpha^2,\ 1 + \alpha + \alpha^2,\ 1 + \alpha^{n/3},\ 1 + \alpha^{2n/3}$, in terms of α to some power, i.e.,

$$
\begin{aligned}
1 + \alpha &= \alpha^{b_1}, \\
1 + \alpha^2 &= (1 + \alpha)^2 = \alpha^{2b_1}, \\
1 + \alpha + \alpha^2 &= \alpha^{b_2}, \\
1 + \alpha^{n/3} &= \alpha^{c_1}, \\
1 + \alpha^{2n/3} &= (1 + \alpha^{n/3})^2 = \alpha^{2c_1}.
\end{aligned}
$$

Rewriting (3.6) and (3.7) respectively as

$$r(\alpha) = \alpha^{a_1}, \alpha^{a_2+b_1}, \alpha^{a_3+2b_1}, \alpha^{a_4+b_2}, \tag{3.8}$$

$$r(\alpha^{n/3}) = \alpha^{na_1/3}, \alpha^{(na_2/3)+c_1}, \alpha^{(na_3/3)+2c_1}, 0. \tag{3.9}$$

The received polynomial r(X) is evaluated at $r(\alpha)$ and $r(\alpha^{n/3})$. We have three possibilities: i) $r(\alpha) = 0$, ii) $r(\alpha) \neq 0$ and $r(\alpha^{n/3}) = 0$ and iii) $r(\alpha) \neq 0$ and $r(\alpha^{n/3}) \neq 0$. Each of these necessarily leads to one or more results.

i) In the event $r(\alpha) = 0$, we have the certitude that no error occurred during transmission.

ii) On the other hand, if $r(\alpha) \neq 0$ and $r(\alpha^{n/3}) = 0$, a burst error of the form $1 + X + X^2$ has occurred starting in position $a_4 + 1$.

iii) Finally, if $r(\alpha) \neq 0$ and $r(\alpha^{n/3}) \neq 0$, then one and only one of the following three equalities must be satisfied:

a) $$r(\alpha^{n/3}) = \alpha^{na_1/3}, \\ = [r(\alpha)]^{n/3}. \tag{3.10}$$

Then a single error, starting in position $a_1 + 1$, has occurred.

b) Or $r(\alpha^{n/3}) = \alpha^{(na_2/3)+c_1} = \alpha^{(na_2/3)+c_1+(nb_1/3)-(nb_1/3)}$,

$= \alpha^{(a_2+b_1)n/3}\ \alpha^{c_1-nb_1/3}$,

$= [r(\alpha)]^{n/3}\ \alpha^{c_1-nb_1/3}$. (3.11)

An error of the form $1 + X$, starting in position $a_2 + 1$, has occurred.

c) Or $r(\alpha^{n/3}) = \alpha^{(na_3/3)+2c_1} = \alpha^{(na_3/3)+(n2b_1/3)+2c_1-n2b_1/3}$,

$= \alpha^{(a_3+2b_1)n/3}\ \alpha^{2(c_1-nb_1/3)}$,

$= [r(\alpha)]^{n/3}\ \alpha^{2(c_1-nb_1/3)}$. (3.12)

An error of the form $1 + X^2$, starting in position $a_3 + 1$, has occurred.

This is, of course, assuming only permissible errors, i.e., bursts of length 3 or less only.

As an example, consider the case where $m = 4$, then $n = 15$. The factor $p(X)$ can be one of the following two primitive polynomials of degree 4: $1 + X + X^4$ and $1 + X^3 + X^4$. Let us focus on the first one. The generator polynomial is given by

$$g(X) = (1 + X + X^4)\ (1 + X + X^2), \text{ or}$$

$$= 1 + X^3 + X^4 + X^5 + X^6.$$

The field representation of $GF(2^4)$ generated by $1 + X + X^4$ is already given above in Table 2.1.

Equations (3.8) and (3.9) become respectively

$$r(\alpha) = \alpha^{a_1}, \alpha^{a_2+4}, \alpha^{a_3+8}, \alpha^{a_4+10}, \text{ and}$$
$$r(\alpha^5) = \alpha^{5a_1}, \alpha^{5a_2+10}, \alpha^{5a_3+5}, 0.$$

Assuming the vector $\{v(X)\} = \{g(X)\}$ is transmitted and we receive

$$r(X) = 1 + X^3 + X^5.$$

Then $r(\alpha) = \alpha^{12}$, and $r(\alpha^5) = \alpha^{10}$. Since $r(\alpha) \neq 0$ and $r(\alpha^5) \neq 0$, an error of the form 1 or $1 + X$ or $1 + X^2$ has occurred. But $[r(\alpha)]^5 = \alpha^{60} = 1$. From iii) c) above,

$$[r(\alpha)]^5 \alpha^{10} = \alpha^{10} = r(\alpha^5).$$

Therefore a burst error of the form $1 + X^2$ has occurred. To find its starting position, we know that $r(\alpha) = \alpha^{12}$. But, with respect to that type of error $(1 + X^2)$, $\alpha^{12} = \alpha^{4+8}$, then $a_3 = 4$, i.e., error starting in position 5. Therefore the error polynomial is $e(X) = X^4 + X^6$, and the transmitted polynomial is

$$\begin{aligned} v(X) &= r(X) + e(X), \\ &= (1 + X^3 + X^5) + (X^4 + X^6), \\ &= 1 + X^3 + X^4 + X^5 + X^6 = g(X). \end{aligned}$$

4. BURST ERROR CORRECTING CAPABILITIES OF CODES

This chapter is devoted to the analysis of the burst error correcting capability of a code that is the null space of

$$h(X) = (1 + X^n) / g(X),$$

where $g(X)$ and $h(X)$ are polynomials with coefficients from GF(2), and $n = 2^q - 1$, q a positive integer. We have mentionned above that for a code of length n, generated by $g(X)$, $h(X)$ can act as a parity check when appropriately used. The following approach is based on the consideration of each $g_i(X)$ and

$$h_i(X) = (1 + X^n) / g_i(X) ,$$

$g_i(X)$ being a factor of $g(X)$, rather than $g(X)$ and $h(X)$ themselves.

This approach brings out interesting results, though it does not produce any startingly new results. Specifically, the approach will be used, by way of illustration, to analyse the case of $1 + X^{31}$ and Abramson codes [14, 15].

4.1. Comments on H^*

Suppose $h_i(X)$ of degree k_i is a factor of $1 + X^n$. Let $h_i^*(X)$ be the reciprocal polynomial of $h_i(X)$ with respect to $n - 1$. Furthermore, let H_i^* be an $(n - k_i)\times(n)$ matrix which has for its rows the binary sequences $\{h_i^*(X)\}$, $\{X^{-1} h_i^*(X)\}$, . . ., $\{X^{-(n-k_i-1)} h_i^*(X)\}$, i.e., $\{h_i^*(X)\}$ and its $n - k_i - 1$ left cyclic shifts. Suppose that

$$h_i(X) = h_{i0} + h_{i1} X + h_{i2} X^2 + \ldots + h_{ik_i} X^{k_i},$$

then the reciprocal polynomial of $h_i(X)$ with respect to $n - 1$ is

$$h_i^*(X) = h_{ik_i} X^{n-k_i-1} + h_{i(k_i-1)} X^{n-k_i} + \ldots + h_{i2} X^{n-3} + h_{i1} X^{n-2} + h_{i0} X^{n-1},$$

therefore

$$\{h_i^*(X)\} = (\overbrace{0 \ \ldots \ 0}^{n-k_i-1} \ h_{ik_i} \ h_{i(k_i-1)} \cdots h_{i2} \ h_{i1} \ h_{i0})$$

and

$$H_i^* = \begin{bmatrix} 0 \ \ldots \ 0 \ h_{ik_i} \ h_{i(k_i-1)} \cdots h_{i2} \ h_{i1} \ h_{i0} \\ 0 \ \ldots \ 0 \ h_{ik_i} \ h_{i(k_i-1)} \cdots h_{i2} \ h_{i1} \ h_{i0} \ 0 \\ \vdots \\ 0 \ h_{ik_i} \ h_{i(k_i-1)} \cdots h_{i2} \ h_{i1} \ h_{i0} \ 0 \ \ldots \ 0 \\ h_{ik_i} \ h_{i(k_i-1)} \cdots h_{i2} \ h_{i1} \ h_{i0} \ 0 \ \ldots \ 0 \end{bmatrix}.$$

Now if we construct a code satisfying the parity check matrices $H_1^*, H_2^*, \ldots, H_s^*$, then:

1) this code is equivalent to the code generated by

$$g(X) = g_1(X)\, g_2(X) \ldots g_s(X)$$

where $g_i(X) = (1 + X^n) / h_i(X)$, and

2) if H^* is the parity check matrix for the code generated by $g(X)$, then, by linear combinations of the appropriate rows of H^*, we can transform H^* into

$$M^* = \begin{bmatrix} H_1^* \\ H_2^* \\ \cdot \\ \cdot \\ \cdot \\ H_s^* \end{bmatrix}.$$

Let us consider, as an example, the case where $n = 15$ and

$g_1(X) = 1 + X + X^4$,

$g_2(X) = 1 + X^3 + X^4$,

$g_3(X) = 1 + X + X^2$.

Then

$g(X) = 1 + X^5 + X^{10}$ and

$h(X) = (1 + X^{15}) / (1 + X^5 + X^{10}) = 1 + X^5$,

$h^*(X) = X^9 + X^{14}$ with respect to $n - 1 = 14$.

H^* is formed of the binary sequence

$$\{h^*(X)\} = (0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1)$$

and its 9 left cyclic shifts.

$$H^* = \begin{bmatrix} 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0 \end{bmatrix} \begin{matrix} \text{------ 1} \\ \text{------ 2} \\ \text{------ 3} \\ \text{------ 4} \\ \text{------ 5} \\ \text{------ 6} \\ \text{------ 7} \\ \text{------ 8} \\ \text{------ 9} \\ \text{------10} \end{matrix}$$

Then it is possible to transform H^* as

$$M^* = \begin{bmatrix} H_1^* \\ \hline H_2^* \\ \hline H_3^* \end{bmatrix}$$

in the following way: if we add to row 1, modulo 2, row 2, row 3, row 4

and row 7 of H^*, we get the following vector:

$$(0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1).$$

The rest of the manipulations are summarized in M^*, where the numbers beside each row of M^* indicate the rows of H^* involved.

$$M^* = \left[\begin{array}{l|l}
0\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1 & 1\ 0\ 2\ 0\ 3\ 0\ 4\ 0\ 7 \\
0\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0 & 2\ 0\ 3\ 0\ 4\ 0\ 5\ 0\ 8 \\
0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0 & 3\ 0\ 4\ 0\ 5\ 0\ 6\ 0\ 9 \\
1\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0 & 4\ 0\ 5\ 0\ 6\ 0\ 7\ 0\ 10 \\
\hline
0\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1 & 1\ 0\ 4\ 0\ 5\ 0\ 6\ 0\ 7 \\
0\ 0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0 & 2\ 0\ 5\ 0\ 6\ 0\ 7\ 0\ 8 \\
0\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0 & 3\ 0\ 6\ 0\ 7\ 0\ 8\ 0\ 9 \\
1\ 1\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 0 & 4\ 0\ 7\ 0\ 8\ 0\ 9\ 0\ 10 \\
\hline
0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 & 1\ 0\ 2\ 0\ 4\ 0\ 5\ 0\ 6\ 0\ 8\ 0\ 9 \\
1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0 & 2\ 0\ 3\ 0\ 5\ 0\ 6\ 0\ 7\ 0\ 9\ 0\ 10
\end{array}\right]$$

But the first row of M^* is the binary sequence of

$$h_1^*(X) = X^3 + X^6 + X^7 + X^9 + X^{11} + X^{12} + X^{13} + X^{14},$$

i.e.,

$$\begin{aligned} h_1(X) &= (1 + X^{15}) \,/\, g_1(X), \\ &= 1 + X + X^2 + X^3 + X^5 + X^7 + X^8 + X^{11}. \end{aligned}$$

Similarly, the fifth row of M^* is the binary sequence of

$$h_2^*(X) = X^3 + X^4 + X^5 + X^6 + X^8 + X^{10} + X^{11} + X^{14},$$

i.e.,

$$h_2(X) = (1 + X^{15}) / g_2(X),$$
$$= 1 + X^3 + X^4 + X^6 + X^8 + X^9 + X^{10} + X^{11}.$$

Finally, the ninth row of M^* is the binary sequence of

$$h_3^*(X) = X + X^2 + X^4 + X^5 + X^7 + X^8 + X^{10} + X^{11} + X^{13} + X^{14},$$

i.e.,

$$h_3(X) = (1 + X^{15}) / g_3(X),$$
$$= 1 + X + X^3 + X^4 + X^6 + X^7 + X^9 + X^{10} + X^{12} + X^{13}.$$

To summarize, the first four rows of M^* are those of H_1^*, i.e., $\{h_1^*(X)\}$ and its three left cyclic shifts. The next four rows of M^* are those of H_2^*, i.e., $\{h_2^*(X)\}$ and its three left cyclic shifts. The last two rows of M^* are those of H_3^*, i.e., $\{h_3^*(X)\}$ and its left cyclic shift.

4.2. Getting the Potential Errors

Any vector $\{v(X)\}$, in the code space V of an (n, k) code, can be expressed as $v(X) = g(X)\, c(X)$ where $g(X)$ is the generator polynomial and $c(X) = \sum_{i=0}^{k-1} c_i X^i$ with coefficients in GF(2).

The received vector $\{r(X)\}$ is a vector in the code space plus an error component $r(X) = v(X) + X^i e(X)$ $i = 0, 1, 2, \ldots, (n - \ell)$, where $e(X) = \sum_{j=0}^{\ell-1} e_j X^j$ with coefficients in GF(2), ℓ being the burst length, $\ell \leq q$ and q satisfies the relation $n = 2^q - 1$.

It can be shown [16] that no code vector of an (n, k) cyclic code is a burst of length $\ell \leq n - k$. Therefore, every (n, k) code can detect any burst of length $\ell \leq n - k$.

If $g_k(X)$ of degree q is the minimum function of α^k then $g_k(\alpha^k) = 0$. Therefore $r(\alpha^k) = \alpha^{i+k} e(\alpha^k)$, $e(\alpha^k)$ can be represented by α to some power in the multiplicative group of $GF(2^q)$.

We will define the set of potential errors in the following way: given a received polynomial, we can decode it only to the extent of being able to say that the error polynomial is

X^{a_1};

$X^{a_2}(1 + X)$;

$X^{a_3}(1 + X^2)$, $X^{a_4}(1 + X + X^2)$;

$X^{a_5}(1 + X^3)$, $X^{a_6}(1 + X + X^3)$, $X^{a_7}(1 + X^2 + X^3)$, $X^{a_8}(1 + X + X^2 + X^3)$;

$X^{a_9}(1 + X^4)$, $X^{a_{10}}(1 + X + X^4)$, ...

.
.
.

$X^{a_{2^{\ell-2}+1}}(1 + X^{\ell-1})$, $X^{a_{2^{\ell-2}+2}}(1 + X + X^{\ell-1})$, ..., OR $X^{a_{2^{\ell-1}}}(1 + X + \ldots + X^{\ell-1})$.

The total number of error polynomials permissible is $2^{\ell-1}$. These polynomials form what we have called the set of potential errors in regards to $g_k(X)$.

4.3. Example 1. Case of $1 + X^{31}$

Let us consider the case where $n = 31$, or equivalently $q = 5$. From the theory of finite field we know that $1 + X^{31}$ has for its factors, $1 + X$ and six primitive polynomials each of degree 5, say $g_1(X)$, $g_2(X)$, $g_3(X)$, $g_4(X)$, $g_5(X)$ and $g_6(X)$. Suppose we wish to find the BEC (Burst Error Correcting) capability of a code generated by $g_i(X)\, g_j(X)$. First, we note that each $g_i(X)$ is a polynomial of degree 5, we can consider only burst of length 5 or less.

The six polynomials [17] referred to are actually:

$g_1(X) = 1 + X^2 + X^5,$

$g_2(X) = 1 + X^3 + X^5,$

$g_3(X) = 1 + X^2 + X^3 + X^4 + X^5,$

$g_4(X) = 1 + X + X^2 + X^3 + X^5,$

$g_5(X) = 1 + X + X^2 + X^4 + X^5,$

$g_6(X) = 1 + X + X^3 + X^4 + X^5.$

The set of potential errors polynomials $E_k(X) = X^{a_k} e_k(X)$, for $\ell \leq 5$, are given in Table 4.1. These are all the possible errors polynomials of burst of length 5 or less.

The received polynomial r(X) can be expressed as $r(X) = g_i(X)\, c(X) + X^j e(X)$ where $X^j e(X)$ is a permissible error polynomial. If α is a primitive element and a root of $g_i(X)$ then $r(\alpha) = \alpha^j e(\alpha)$. Referring to the tables of field elements (Table 4.2 to Table 4.7) gotten through $g_i(X)$, we can express $e(\alpha)$ as α to some power for each correctable error pattern.

Table 4.1. Set of Potential Error Polynomials for $\ell \leq 5$

$E_k(X)$	X^{a_k}	$e_k(X)$	$\{e_k(X)\}$
$E_1(X)$	X^{a_1}	(1)	(1 0 0 0 0)
$E_2(X)$	X^{a_2}	$(1 + X)$	(1 1 0 0 0)
$E_3(X)$	X^{a_3}	$(1 + X^2)$	(1 0 1 0 0)
$E_4(X)$	X^{a_4}	$(1 + X + X^2)$	(1 1 1 0 0)
$E_5(X)$	X^{a_5}	$(1 + X^3)$	(1 0 0 1 0)
$E_6(X)$	X^{a_6}	$(1 + X + X^3)$	(1 1 0 1 0)
$E_7(X)$	X^{a_7}	$(1 + X^2 + X^3)$	(1 0 1 1 0)
$E_8(X)$	X^{a_8}	$(1 + X + X^2 + X^3)$	(1 1 1 1 0)
$E_9(X)$	X^{a_9}	$(1 + X^4)$	(1 0 0 0 1)
$E_{10}(X)$	$X^{a_{10}}$	$(1 + X + X^4)$	(1 1 0 0 1)
$E_{11}(X)$	$X^{a_{11}}$	$(1 + X^2 + X^4)$	(1 0 1 0 1)
$E_{12}(X)$	$X^{a_{12}}$	$(1 + X + X^2 + X^4)$	(1 1 1 0 1)
$E_{13}(X)$	$X^{a_{13}}$	$(1 + X^3 + X^4)$	(1 0 0 1 1)
$E_{14}(X)$	$X^{a_{14}}$	$(1 + X + X^3 + X^4)$	(1 1 0 1 1)
$E_{15}(X)$	$X^{a_{15}}$	$(1 + X^2 + X^3 + X^4)$	(1 0 1 1 1)
$E_{16}(X)$	$X^{a_{16}}$	$(1 + X + X^2 + X^3 + X^4)$	(1 1 1 1 1)

Table 4.2. Field Elements Representation of GF(2^5)

Generated by $g_1(X) = 1 + X^2 + X^5$

α^0	$= 1$	$= (1\ 0\ 0\ 0\ 0)$
α^1	$= \alpha$	$= (0\ 1\ 0\ 0\ 0)$
α^2	$= \alpha^2$	$= (0\ 0\ 1\ 0\ 0)$
α^3	$= \alpha^3$	$= (0\ 0\ 0\ 1\ 0)$
α^4	$= \alpha^4$	$= (0\ 0\ 0\ 0\ 1)$
α^5	$= 1 + \alpha^2$	$= (1\ 0\ 1\ 0\ 0)$
α^6	$= \alpha + \alpha^3$	$= (0\ 1\ 0\ 1\ 0)$
α^7	$= \alpha^2 + \alpha^4$	$= (0\ 0\ 1\ 0\ 1)$
α^8	$= 1 + \alpha^2 + \alpha^3$	$= (1\ 0\ 1\ 1\ 0)$
α^9	$= \alpha + \alpha^3 + \alpha^4$	$= (0\ 1\ 0\ 1\ 1)$
α^{10}	$= 1 + \alpha^4$	$= (1\ 0\ 0\ 0\ 1)$
α^{11}	$= 1 + \alpha + \alpha^2$	$= (1\ 1\ 1\ 0\ 0)$
α^{12}	$= \alpha + \alpha^2 + \alpha^3$	$= (0\ 1\ 1\ 1\ 0)$
α^{13}	$= \alpha^2 + \alpha^3 + \alpha^4$	$= (0\ 0\ 1\ 1\ 1)$
α^{14}	$= 1 + \alpha^2 + \alpha^3 + \alpha^4$	$= (1\ 0\ 1\ 1\ 1)$
α^{15}	$= 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	$= (1\ 1\ 1\ 1\ 1)$

Table 4.2. (continued)

$\alpha^{16} = 1 + \alpha + \alpha^3 + \alpha^4 = (1\ 1\ 0\ 1\ 1)$

$\alpha^{17} = 1 + \alpha + \alpha^4 = (1\ 1\ 0\ 0\ 1)$

$\alpha^{18} = 1 + \alpha = (1\ 1\ 0\ 0\ 0)$

$\alpha^{19} = \alpha + \alpha^2 = (0\ 1\ 1\ 0\ 0)$

$\alpha^{20} = \alpha^2 + \alpha^3 = (0\ 0\ 1\ 1\ 0)$

$\alpha^{21} = \alpha^3 + \alpha^4 = (0\ 0\ 0\ 1\ 1)$

$\alpha^{22} = 1 + \alpha^2 + \alpha^4 = (1\ 0\ 1\ 0\ 1)$

$\alpha^{23} = 1 + \alpha + \alpha^2 + \alpha^3 = (1\ 1\ 1\ 1\ 0)$

$\alpha^{24} = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (0\ 1\ 1\ 1\ 1)$

$\alpha^{25} = 1 + \alpha^3 + \alpha^4 = (1\ 0\ 0\ 1\ 1)$

$\alpha^{26} = 1 + \alpha + \alpha^2 + \alpha^4 = (1\ 1\ 1\ 0\ 1)$

$\alpha^{27} = 1 + \alpha + \alpha^3 = (1\ 1\ 0\ 1\ 0)$

$\alpha^{28} = \alpha + \alpha^2 + \alpha^4 = (0\ 1\ 1\ 0\ 1)$

$\alpha^{29} = 1 + \alpha^3 = (1\ 0\ 0\ 1\ 0)$

$\alpha^{30} = \alpha + \alpha^4 = (0\ 1\ 0\ 0\ 1)$

$\alpha^{31} = 1 = \alpha^0$

Table 4.3. Field Elements Representation of $GF(2^5)$ Generated by $g_2(X) = 1 + X^3 + X^5$

α^0	$= 1$	$= (1\ 0\ 0\ 0\ 0)$
α^1	$= \alpha$	$= (0\ 1\ 0\ 0\ 0)$
α^2	$= \alpha^2$	$= (0\ 0\ 1\ 0\ 0)$
α^3	$= \alpha^3$	$= (0\ 0\ 0\ 1\ 0)$
α^4	$= \alpha^4$	$= (0\ 0\ 0\ 0\ 1)$
α^5	$= 1 + \alpha^3$	$= (1\ 0\ 0\ 1\ 0)$
α^6	$= \alpha + \alpha^4$	$= (0\ 1\ 0\ 0\ 1)$
α^7	$= 1 + \alpha^2 + \alpha^3$	$= (1\ 0\ 1\ 1\ 0)$
α^8	$= \alpha + \alpha^3 + \alpha^4$	$= (0\ 1\ 0\ 1\ 1)$
α^9	$= 1 + \alpha^2 + \alpha^3 + \alpha^4$	$= (1\ 0\ 1\ 1\ 1)$
α^{10}	$= 1 + \alpha + \alpha^4$	$= (1\ 1\ 0\ 0\ 1)$
α^{11}	$= 1 + \alpha + \alpha^2 + \alpha^3$	$= (1\ 1\ 1\ 1\ 0)$
α^{12}	$= \alpha + \alpha^2 + \alpha^3 + \alpha^4$	$= (0\ 1\ 1\ 1\ 1)$
α^{13}	$= 1 + \alpha^2 + \alpha^4$	$= (1\ 0\ 1\ 0\ 1)$
α^{14}	$= 1 + \alpha$	$= (1\ 1\ 0\ 0\ 0)$
α^{15}	$= \alpha + \alpha^2$	$= (0\ 1\ 1\ 0\ 0)$

Table 4.3. (continued)

$\alpha^{16} = \alpha^2 + \alpha^3 = (0\ 0\ 1\ 1\ 0)$

$\alpha^{17} = \alpha^3 + \alpha^4 = (0\ 0\ 0\ 1\ 1)$

$\alpha^{18} = 1 + \alpha^3 + \alpha^4 = (1\ 0\ 0\ 1\ 1)$

$\alpha^{19} = 1 + \alpha + \alpha^3 + \alpha^4 = (1\ 1\ 0\ 1\ 1)$

$\alpha^{20} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 1\ 1\ 1\ 1)$

$\alpha^{21} = 1 + \alpha + \alpha^2 + \alpha^4 = (1\ 1\ 1\ 0\ 1)$

$\alpha^{22} = 1 + \alpha + \alpha^2 = (1\ 1\ 1\ 0\ 0)$

$\alpha^{23} = \alpha + \alpha^2 + \alpha^3 = (0\ 1\ 1\ 1\ 0)$

$\alpha^{24} = \alpha^2 + \alpha^3 + \alpha^4 = (0\ 0\ 1\ 1\ 1)$

$\alpha^{25} = 1 + \alpha^4 = (1\ 0\ 0\ 0\ 1)$

$\alpha^{26} = 1 + \alpha + \alpha^3 = (1\ 1\ 0\ 1\ 0)$

$\alpha^{27} = \alpha + \alpha^2 + \alpha^4 = (0\ 1\ 1\ 0\ 1)$

$\alpha^{28} = 1 + \alpha^2 = (1\ 0\ 1\ 0\ 0)$

$\alpha^{29} = \alpha + \alpha^3 = (0\ 1\ 0\ 1\ 0)$

$\alpha^{30} = \alpha^2 + \alpha^4 = (0\ 0\ 1\ 0\ 1)$

$\alpha^{31} = 1 = \alpha^0$

Table 4.4. Field Elements Representation of GF(2^5)
Generated by $g_3(X) = 1 + X^2 + X^3 + X^4 + X^5$

α^0	$= 1$	$= (1\ 0\ 0\ 0\ 0)$
α^1	$= \alpha$	$= (0\ 1\ 0\ 0\ 0)$
α^2	$= \alpha^2$	$= (0\ 0\ 1\ 0\ 0)$
α^3	$= \alpha^3$	$= (0\ 0\ 0\ 1\ 0)$
α^4	$= \alpha^4$	$= (0\ 0\ 0\ 0\ 1)$
α^5	$= 1 + \alpha^2 + \alpha^3 + \alpha^4$	$= (1\ 0\ 1\ 1\ 1)$
α^6	$= 1 + \alpha + \alpha^2$	$= (1\ 1\ 1\ 0\ 0)$
α^7	$= \alpha + \alpha^2 + \alpha^3$	$= (0\ 1\ 1\ 1\ 0)$
α^8	$= \alpha^2 + \alpha^3 + \alpha^4$	$= (0\ 0\ 1\ 1\ 1)$
α^9	$= 1 + \alpha^2$	$= (1\ 0\ 1\ 0\ 0)$
α^{10}	$= \alpha + \alpha^3$	$= (0\ 1\ 0\ 1\ 0)$
α^{11}	$= \alpha^2 + \alpha^4$	$= (0\ 0\ 1\ 0\ 1)$
α^{12}	$= 1 + \alpha^2 + \alpha^4$	$= (1\ 0\ 1\ 0\ 1)$
α^{13}	$= 1 + \alpha + \alpha^2 + \alpha^4$	$= (1\ 1\ 1\ 0\ 1)$
α^{14}	$= 1 + \alpha + \alpha^4$	$= (1\ 1\ 0\ 0\ 1)$
α^{15}	$= 1 + \alpha + \alpha^3 + \alpha^4$	$= (1\ 1\ 0\ 1\ 1)$

Table 4.4. (continued)

$\alpha^{16} = 1 + \alpha + \alpha^3 = (1\ 1\ 0\ 1\ 0)$

$\alpha^{17} = \alpha + \alpha^2 + \alpha^4 = (0\ 1\ 1\ 0\ 1)$

$\alpha^{18} = 1 + \alpha^4 = (1\ 0\ 0\ 0\ 1)$

$\alpha^{19} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 1\ 1\ 1\ 1)$

$\alpha^{20} = 1 + \alpha = (1\ 1\ 0\ 0\ 0)$

$\alpha^{21} = \alpha + \alpha^2 = (0\ 1\ 1\ 0\ 0)$

$\alpha^{22} = \alpha^2 + \alpha^3 = (0\ 0\ 1\ 1\ 0)$

$\alpha^{23} = \alpha^3 + \alpha^4 = (0\ 0\ 0\ 1\ 1)$

$\alpha^{24} = 1 + \alpha^2 + \alpha^3 = (1\ 0\ 1\ 1\ 0)$

$\alpha^{25} = \alpha + \alpha^3 + \alpha^4 = (0\ 1\ 0\ 1\ 1)$

$\alpha^{26} = 1 + \alpha^3 = (1\ 0\ 0\ 1\ 0)$

$\alpha^{27} = \alpha + \alpha^4 = (0\ 1\ 0\ 0\ 1)$

$\alpha^{28} = 1 + \alpha^3 + \alpha^4 = (1\ 0\ 0\ 1\ 1)$

$\alpha^{29} = 1 + \alpha + \alpha^2 + \alpha^3 = (1\ 1\ 1\ 1\ 0)$

$\alpha^{30} = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (0\ 1\ 1\ 1\ 1)$

$\alpha^{31} = 1 = \alpha^0$

Table 4.5. Field Elements Representation of $GF(2^5)$

Generated by $g_4(X) = 1 + X + X^2 + X^3 + X^5$

α^0	$= 1$	$= (1\ 0\ 0\ 0\ 0)$
α^1	$= \alpha$	$= (0\ 1\ 0\ 0\ 0)$
α^2	$= \alpha^2$	$= (0\ 0\ 1\ 0\ 0)$
α^3	$= \alpha^3$	$= (0\ 0\ 0\ 1\ 0)$
α^4	$= \alpha^4$	$= (0\ 0\ 0\ 0\ 1)$
α^5	$= 1 + \alpha + \alpha^2 + \alpha^3$	$= (1\ 1\ 1\ 1\ 0)$
α^6	$= \alpha + \alpha^2 + \alpha^3 + \alpha^4$	$= (0\ 1\ 1\ 1\ 1)$
α^7	$= 1 + \alpha + \alpha^4$	$= (1\ 1\ 0\ 0\ 1)$
α^8	$= 1 + \alpha^3$	$= (1\ 0\ 0\ 1\ 0)$
α^9	$= \alpha + \alpha^4$	$= (0\ 1\ 0\ 0\ 1)$
α^{10}	$= 1 + \alpha + \alpha^3$	$= (1\ 1\ 0\ 1\ 0)$
α^{11}	$= \alpha + \alpha^2 + \alpha^4$	$= (0\ 1\ 1\ 0\ 1)$
α^{12}	$= 1 + \alpha$	$= (1\ 1\ 0\ 0\ 0)$
α^{13}	$= \alpha + \alpha^2$	$= (0\ 1\ 1\ 0\ 0)$
α^{14}	$= \alpha^2 + \alpha^3$	$= (0\ 0\ 1\ 1\ 0)$
α^{15}	$= \alpha^3 + \alpha^4$	$= (0\ 0\ 0\ 1\ 1)$

Table 4.5. (continued)

$\alpha^{16} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 1\ 1\ 1\ 1)$

$\alpha^{17} = 1 + \alpha^4 = (1\ 0\ 0\ 0\ 1)$

$\alpha^{18} = 1 + \alpha^2 + \alpha^3 = (1\ 0\ 1\ 1\ 0)$

$\alpha^{19} = \alpha + \alpha^3 + \alpha^4 = (0\ 1\ 0\ 1\ 1)$

$\alpha^{20} = 1 + \alpha + \alpha^3 + \alpha^4 = (1\ 1\ 0\ 1\ 1)$

$\alpha^{21} = 1 + \alpha^3 + \alpha^4 = (1\ 0\ 0\ 1\ 1)$

$\alpha^{22} = 1 + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 0\ 1\ 1\ 1)$

$\alpha^{23} = 1 + \alpha^2 + \alpha^4 = (1\ 0\ 1\ 0\ 1)$

$\alpha^{24} = 1 + \alpha^2 = (1\ 0\ 1\ 0\ 0)$

$\alpha^{25} = \alpha + \alpha^3 = (0\ 1\ 0\ 1\ 0)$

$\alpha^{26} = \alpha^2 + \alpha^4 = (0\ 0\ 1\ 0\ 1)$

$\alpha^{27} = 1 + \alpha + \alpha^2 = (1\ 1\ 1\ 0\ 0)$

$\alpha^{28} = \alpha + \alpha^2 + \alpha^3 = (0\ 1\ 1\ 1\ 0)$

$\alpha^{29} = \alpha^2 + \alpha^3 + \alpha^4 = (0\ 0\ 1\ 1\ 1)$

$\alpha^{30} = 1 + \alpha + \alpha^2 + \alpha^4 = (1\ 1\ 1\ 0\ 1)$

$\alpha^{31} = 1 = \alpha^0$

Table 4.6. Field Elements Representation of $GF(2^5)$ Generated by $g_1(X) = 1 + X + X^2 + X^4 + X^5$

α^0	$= 1$	$= (1\ 0\ 0\ 0\ 0)$
α^1	$= \alpha$	$= (0\ 1\ 0\ 0\ 0)$
α^2	$= \alpha^2$	$= (0\ 0\ 1\ 0\ 0)$
α^3	$= \alpha^3$	$= (0\ 0\ 0\ 1\ 0)$
α^4	$= \alpha^4$	$= (0\ 0\ 0\ 0\ 1)$
α^5	$= 1 + \alpha + \alpha^2 + \alpha^4$	$= (1\ 1\ 1\ 0\ 1)$
α^6	$= 1 + \alpha^3 + \alpha^4$	$= (1\ 0\ 0\ 1\ 1)$
α^7	$= 1 + \alpha^2$	$= (1\ 0\ 1\ 0\ 0)$
α^8	$= \alpha + \alpha^3$	$= (0\ 1\ 0\ 1\ 0)$
α^9	$= \alpha^2 + \alpha^4$	$= (0\ 0\ 1\ 0\ 1)$
α^{10}	$= 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4$	$= (1\ 1\ 1\ 1\ 1)$
α^{11}	$= 1 + \alpha^3$	$= (1\ 0\ 0\ 1\ 0)$
α^{12}	$= \alpha + \alpha^4$	$= (0\ 1\ 0\ 0\ 1)$
α^{13}	$= 1 + \alpha + \alpha^4$	$= (1\ 1\ 0\ 0\ 1)$
α^{14}	$= 1 + \alpha^4$	$= (1\ 0\ 0\ 0\ 1)$
α^{15}	$= 1 + \alpha^2 + \alpha^4$	$= (1\ 0\ 1\ 0\ 1)$

Table 4.6. (continued)

$\alpha^{16} = 1 + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 0\ 1\ 1\ 1)$

$\alpha^{17} = 1 + \alpha^2 + \alpha^3 + = (1\ 0\ 1\ 1\ 0)$

$\alpha^{18} = \alpha + \alpha^3 + \alpha^4 = (0\ 1\ 0\ 1\ 1)$

$\alpha^{19} = 1 + \alpha + = (1\ 1\ 0\ 0\ 0)$

$\alpha^{20} = \alpha + \alpha^2 = (0\ 1\ 1\ 0\ 0)$

$\alpha^{21} = \alpha^2 + \alpha^3 = (0\ 0\ 1\ 1\ 0)$

$\alpha^{22} = \alpha^3 + \alpha^4 = (0\ 0\ 0\ 1\ 1)$

$\alpha^{23} = 1 + \alpha + \alpha^2 = (1\ 1\ 1\ 0\ 0)$

$\alpha^{24} = \alpha + \alpha^2 + \alpha^3 = (0\ 1\ 1\ 1\ 0)$

$\alpha^{25} = \alpha^2 + \alpha^3 + \alpha^4 = (0\ 0\ 1\ 1\ 1)$

$\alpha^{26} = 1 + \alpha + \alpha^2 + \alpha^3 = (1\ 1\ 1\ 1\ 0)$

$\alpha^{27} = \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (0\ 1\ 1\ 1\ 1)$

$\alpha^{28} = 1 + \alpha + \alpha^3 = (1\ 1\ 0\ 1\ 0)$

$\alpha^{29} = \alpha + \alpha^2 + \alpha^4 = (0\ 1\ 1\ 0\ 1)$

$\alpha^{30} = 1 + \alpha + \alpha^3 + \alpha^4 = (1\ 1\ 0\ 1\ 1)$

$\alpha^{31} = 1 = \alpha^0$

Table 4.7. Field Elements Representation of GF(2^5)

Generated by $g_6(X) = 1 + X + X^3 + X^4 + X^5$

α^0	$= 1$	$= (1\ 0\ 0\ 0\ 0)$
α^1	$= \alpha$	$= (0\ 1\ 0\ 0\ 0)$
α^2	$= \alpha^2$	$= (0\ 0\ 1\ 0\ 0)$
α^3	$= \alpha^3$	$= (0\ 0\ 0\ 1\ 0)$
α^4	$= \alpha^4$	$= (0\ 0\ 0\ 0\ 1)$
α^5	$= 1 + \alpha + \alpha^3 + \alpha^4$	$= (1\ 1\ 0\ 1\ 1)$
α^6	$= 1 + \alpha^2 + \alpha^3$	$= (1\ 0\ 1\ 1\ 0)$
α^7	$= \alpha + \alpha^3 + \alpha^4$	$= (0\ 1\ 0\ 1\ 1)$
α^8	$= 1 + \alpha + \alpha^2 + \alpha^3$	$= (1\ 1\ 1\ 1\ 0)$
α^9	$= \alpha + \alpha^2 + \alpha^3 + \alpha^4$	$= (0\ 1\ 1\ 1\ 1)$
α^{10}	$= 1 + \alpha + \alpha^2$	$= (1\ 1\ 1\ 0\ 0)$
α^{11}	$= \alpha + \alpha^2 + \alpha^3$	$= (0\ 1\ 1\ 1\ 0)$
α^{12}	$= \alpha^2 + \alpha^3 + \alpha^4$	$= (0\ 0\ 1\ 1\ 1)$
α^{13}	$= 1 + \alpha$	$= (1\ 1\ 0\ 0\ 0)$
α^{14}	$= \alpha + \alpha^2$	$= (0\ 1\ 1\ 0\ 0)$
α^{15}	$= \alpha^2 + \alpha^3$	$= (0\ 0\ 1\ 1\ 0)$

Table 4.7. (continued)

$\alpha^{16} = \alpha^3 + \alpha^4 = (0\ 0\ 0\ 1\ 1)$

$\alpha^{17} = 1 + \alpha + \alpha^3 = (1\ 1\ 0\ 1\ 0)$

$\alpha^{18} = \alpha + \alpha^2 + \alpha^4 = (0\ 1\ 1\ 0\ 1)$

$\alpha^{19} = 1 + \alpha + \alpha^2 + \alpha^4 = (1\ 1\ 1\ 0\ 1)$

$\alpha^{20} = 1 + \alpha^2 + \alpha^4 = (1\ 0\ 1\ 0\ 1)$

$\alpha^{21} = 1 + \alpha^4 = (1\ 0\ 0\ 0\ 1)$

$\alpha^{22} = 1 + \alpha^3 + \alpha^4 = (1\ 0\ 0\ 1\ 1)$

$\alpha^{23} = 1 + \alpha^3 = (1\ 0\ 0\ 1\ 0)$

$\alpha^{24} = \alpha + \alpha^4 = (0\ 1\ 0\ 0\ 1)$

$\alpha^{25} = 1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 1\ 1\ 1\ 1)$

$\alpha^{26} = 1 + \alpha^2 = (1\ 0\ 1\ 0\ 0)$

$\alpha^{27} = \alpha + \alpha^3 = (0\ 1\ 0\ 1\ 0)$

$\alpha^{28} = \alpha^2 + \alpha^4 = (0\ 0\ 1\ 0\ 1)$

$\alpha^{29} = 1 + \alpha + \alpha^4 = (1\ 1\ 0\ 0\ 1)$

$\alpha^{30} = 1 + \alpha^2 + \alpha^3 + \alpha^4 = (1\ 0\ 1\ 1\ 1)$

$\alpha^{31} = 1 = \alpha^0$

Next, we find where each error pattern should start, i.e., find j in $\alpha^j e(\alpha)$, so that we get the same power of α for each error pattern. Since, within the same error pattern the syndromes are all distinct, i.e., $S = \{\alpha^i \sum_{k=0}^{\ell-1} e_k X^k\} H^{*T}$ are all distinct for all i = 0, 1, 2, ... , n - ℓ, and for errors of different pattern it is possible to find an i and a j, such that

$$X^i e_1(X) = X^j e_2(X)$$

where the degree of $e_1(X)$ = degree of $e_2(X)$. Then $E_1(\alpha) = \ldots = E_{16}(\alpha)$.

In regard to $g_1(X)$, $E_2(\alpha) = \alpha^{a_2} (1 + \alpha) = \alpha^{a_2+18}$ from Table 4.2. But $E_2(\alpha) = E_1(\alpha)$, then $\alpha^{a_2+18} = \alpha^{a_1}$. Therefore $\alpha^{a_2} = \alpha^{a_1+13}$ and $E_2(\alpha) = \alpha^{a_1+13} (1 + \alpha)$. Similarly for the other error patterns:

$E_3(\alpha) = \alpha^{a_1+26} (1 + \alpha^2)$, $E_4(\alpha) = \alpha^{a_1+20} (1 + \alpha + \alpha^2)$;

$E_5(\alpha) = \alpha^{a_1+2} (1 + \alpha^3)$, $E_6(\alpha) = \alpha^{a_1+4} (1 + \alpha + \alpha^3)$,

$E_7(\alpha) = \alpha^{a_1+23} (1 + \alpha^2 + \alpha^3)$, $E_8(\alpha) = \alpha^{a_1+8} (1 + \alpha + \alpha^2 + \alpha^3)$;

$E_9(\alpha) = \alpha^{a_1+21} (1 + \alpha^4)$, $E_{10}(\alpha) = \alpha^{a_1+14} (1 + \alpha + \alpha^4)$,

$E_{11}(\alpha) = \alpha^{a_1+9} (1 + \alpha^2 + \alpha^4)$, $E_{12}(\alpha) = \alpha^{a_1+5} (1 + \alpha + \alpha^2 + \alpha^4)$,

$E_{13}(\alpha) = \alpha^{a_1+6} (1 + \alpha^3 + \alpha^4)$, $E_{14}(\alpha) = \alpha^{a_1+15} (1 + \alpha + \alpha^3 + \alpha^4)$,

$E_{15}(\alpha) = \alpha^{a_1+17} (1 + \alpha^2 + \alpha^3 + \alpha^4)$, $E_{16}(\alpha) = \alpha^{a_1+16} (1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4)$.

This complete the process of getting the set of potential errors. The process is repeated for each $g_i(X)$.

After getting the set of potential errors for each $g_i(X)$ we form Table 4.8. In this table the entries are the starting positions of all acceptable errors. Also in this table g_i means $g_i(X)$ and e_j means $e_j(X)$, the error pattern. For instance e_4 refers to the pattern $(1 + X + X^2)$ of Table 4.1. To indicate what the entries in each of these rows mean, we may mention that the entries in row g_1, for example, are the same powers of α plus 1 in the set of potential errors given earlier for the case of $g_1(X)$ a_1 being normalized to zero. This table says that, considering row g_1, an error of type, say e_7 starting in position 24, will "match" (will not be distinguishable from) with an error of type, say e_{12} starting in position 6.

To show how to use this table, let us consider row g_1 and g_2. The entries under e_1 are the same for g_1 and g_2 and the other entries under e_k, $k = 2, 3, \ldots, 16$ are different, i.e., an error of type e_1 will not "match" with any other error patterns. Now we make the entries under e_2 the same by adding 4 (mod 31) to all entries in row g_1 such that we get:

g_1 : 5; 18; 31, 25; 7, 8, 29, 13; 26, 19, 14, 10, 11, 20, 22, 21; and

g_2 : 1; 18; 4, 10; 27, 6, 25, 21; 7, 22, 19, 11, 15, 13, 23, 12.

Again, here, an error pattern of the type e_2 will not "match" with any other error pattern. The process is repeated for the other error patterns. This is summarized in Table 4.9.

Table ..., Error Starting Position.

Burst Length	1	2	3		4				5							
Error Pattern / Poly-nomial	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}
g_1	1	14	27	21	3	5	24	9	22	15	10	6	7	16	18	17
g_2	1	18	4	10	27	6	25	21	7	22	19	11	14	13	23	12
g_3	1	12	23	26	6	16	8	3	14	18	20	19	4	17	27	13
g_4	1	20	8	5	24	22	14	27	15	25	9	2	11	12	10	16
g_5	1	13	25	9	21	4	15	6	18	19	17	27	26	2	16	22
g_6	1	19	6	22	9	15	26	24	11	3	12	13	10	27	2	7

Table 4.9. Comparison of $g_1(X)$ and $g_2(X)$

ROWS	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}
1	1 1	14 18	27 4	21 10	3 27	5 6	24 25	9 21	22 7	15 22	10 19	6 11	7 14	16 13	18 23	17 12
2	5 1	18 18	3 4	25 10	7 27	9 6	28 25	13 21	26 7	19 22	14 19	10 11	11 14	20 13	22 23	21 12
3	9 1	22 18	4 4	29 10	11 27	13 6	1 25	17 21	30 7	23 22	18 19	14 11	15 14	24 13	26 23	25 12
4	1 12	14 29	27 15	21 21	3 7	5 17	24 5	9 1	22 18	15 2	10 30	6 22	7 25	16 24	18 3	17 23
5	1 8	14 29	27 21	21 17	3 3	5 13	24 22	9 28	22 14	15 29	10 26	6 18	7 21	16 20	18 30	17 19
6	2 1	15 18	28 4	22 10	4 27	6 6	25 25	10 21	23 7	16 22	11 19	7 11	8 14	17 13	19 23	18 12
7	13 1	26 18	7 4	8 10	15 27	17 6	5 25	21 21	3 7	27 22	22 19	18 11	19 14	28 13	30 23	29 12
8	1 16	14 2	27 19	21 25	3 11	5 21	24 9	9 5	22 22	15 6	10 3	6 26	7 29	16 28	18 7	17 27
9	8 1	21 18	3 4	28 10	10 27	12 6	31 25	16 21	29 7	22 22	17 19	13 11	14 14	23 13	25 23	24 12
10	10 1	23 18	5 4	30 10	12 27	4 6	2 25	18 21	31 7	24 22	19 19	15 11	16 14	25 13	27 23	26 12
11	6 1	19 18	1 4	26 10	8 27	10 6	29 25	14 21	27 7	20 22	15 19	11 11	12 14	21 13	23 23	22 12
12	1 4	14 21	27 7	21 13	3 30	5 9	24 28	9 24	22 10	15 25	10 22	6 14	7 17	16 16	18 26	17 15
13	1 6	14 23	27 9	21 15	3 1	5 11	24 30	9 26	22 12	15 27	10 24	6 16	7 19	16 18	18 28	17 17

The analysis of Table 4.9 is as follows: the entries in, say, row 6, column e_6 were made equal by adding 1 (mod 31) to row g_1 of Table 4.8. In doing so, the entries under column e_7 were equalled. This means that error patterns of type e_6 and e_7 are not distinguishable, i.e., the code generated by $g_1(X)\ g_2(X)$ can correct either the error pattern $1 + X + X^3$ or $1 + X^2 + X^3$ but not both. Similarly for row 9, the code can correct either the error pattern $1 + X + X^4$ or $1 + X^3 + X^4$. And finally for row 11, the code can correct either the error pattern $1 + X + X^2 + X^4$ or $1 + X^2 + X^3 + X^4$.

The process for getting Table 4.9 would be long if we are to consider all possible $g_i(X)\ g_j(X)$. Table 4.9 can be further condensed by subtracting (mod 31), entry-by-entry, row g_2 from row g_1 of Table 4.8. Then we get the sequence: 0; 27; 23, 11; 7, 30, 30, 19; 15, 24, 22, 26, 24, 3, 26, 5. In this sequence we see that there are a few numbers which are repeated: 30, 24, 26. The analysis is the same as for Table 4.9, therefore, we can say that the code generated by $g_1(X)\ g_2(X)$ can correct single errors, bursts of length 2, bursts of length 3, bursts of length 4 except $1 + X + X^3$ or $1 + X^2 + X^3$, and bursts of length 5 except $1 + X + X^4$ or $1 + X^3 + X^4$ and $1 + X + X^2 + X^4$ or $1 + X^2 + X^3 + X^4$.

From a practical point of view it is, of course, unrealistic to say that a particular pattern of error will not occur in regards to a certain burst length. In this sense we have to exclude bursts of length 4 and 5. So we can finally say that the code generated by $g_1(X)\ g_2(X)$ can

correct all bursts of length 3 or less. On the other hand, if we consider only solid bursts, the code can correct all solid bursts of length 5 or less. Table 4.9 was included to show the process in which the method was developed.

The discussion of the preceding paragraph has been epitomized in Table 4.10 which also includes other pairwise combinations of $g_i(X)$'s. This table is derived from Table 4.8. Thus the first row $g_1 g_2$, in Table 4.10, represents the entry-by-entry difference (mod 31) of row g_1 and g_2 of Table 4.8 and corresponds to the code generated by $g_1(X)\ g_2(X)$. This is indicated by $g_1 g_2$ in column entitled "generator" in Table 4.10.

With the aid of Table 4.10, we can easily arrive at the BEC capability. For instance, the code generated by $g_3(X)\ g_5(X)$ in regards to row $g_3 g_5$, can correct all bursts of length 4 or less. We have to exclude bursts of length 5 because 30 appears twice: once in regards to burst of length 2 and second in regards to burst of length 5. So we have to omit one of these two situations. From a practical point of view, it is more realistic to exclude the latter. However, it is interesting to note, as a special case, that solid bursts of length 5 can be included though it is unrealistic.

Table 4.10. Entry-by-entry Difference of any Two Rows of Table 4.8

Burst Length	1	2	3		4				5							
Error Pattern / Generator	e_1	e_2	e_3	e_4	e_5	e_6	e_7	e_8	e_9	e_{10}	e_{11}	e_{12}	e_{13}	e_{14}	e_{15}	e_{16}
$g_1 g_2$	0	27	23	11	7	(30)	(30)	19	15	[24]	22	△26	[24]	3	△26	5
$g_1 g_3$	0	2	4	26	28	20	16	6	8	28	21	18	3	30	22	4
$g_1 g_4$	0	25	19	16	10	14	10	13	7	21	1	4	27	4	8	1
$g_1 g_5$	0	1	2	12	13	1	9	3	4	27	24	10	12	14	2	26
$g_1 g_6$	0	26	21	30	25	21	29	16	11	12	29	24	28	20	16	10
$g_2 g_3$	0	6	12	15	21	21	17	18	24	4	30	23	10	27	27	30
$g_2 g_4$	0	29	27	5	3	15	11	25	23	28	10	9	3	1	13	27
$g_2 g_5$	0	5	10	1	6	2	10	15	20	3	2	15	19	11	7	21
$g_2 g_6$	0	30	29	19	18	22	30	28	27	19	7	29	4	17	21	5
$g_3 g_4$	0	23	15	21	13	25	25	7	30	24	11	17	24	5	17	28
$g_3 g_5$	0	30	29	17	16	12	24	28	27	30	3	23	9	15	11	22
$g_3 g_6$	0	24	17	14	28	1	13	10	3	15	8	6	25	21	25	6
$g_4 g_5$	0	7	14	27	3	18	30	21	28	6	23	6	16	10	25	25
$g_4 g_6$	0	1	2	14	15	7	19	3	4	22	28	20	1	16	8	9
$g_5 g_6$	0	25	19	18	12	20	20	13	7	16	5	14	16	6	14	15

Examination of Table 4.10 shows that the codes generated by $g_1(X)\ g_2(X)$, $g_1(X)\ g_4(X)$, $g_1(X)\ g_5(X)$, $g_1(X)\ g_6(X)$, $g_2(X)\ g_3(X)$, $g_2(X)\ g_5(X)$, $g_2(X)\ g_6(X)$, $g_3(X)\ g_4(X)$, $g_5(X)\ g_6(X)$ can each correct all bursts of length 3 or less whereas the codes generated by $g_1(X)\ g_3(X)$, $g_2(X)\ g_4(X)$, $g_3(X)\ g_5(X)$, $g_3(X)\ g_6(X)$, $g_4(X)\ g_5(X)$, $g_4(X)\ g_6(X)$ can each correct all bursts of length 4 or less. Thus the latter are superior to the former.

It is clear from the discussion so far in this section, that the main step is to get the set of potential errors for each $g_i(X)$. Once we have these sets, getting the BEC capability of each $g_i(X)\ g_j(X)$, $i \neq j$, is extremely simple. This procedure is much simpler than examination of the parity check matrix H^* for each $g(X) = g_i(X)\ g_j(X)$.

We now go one step further and investigate the BEC capability of the product $g_i(X)$, $g_j(X)$ and $g_k(X)$, i.e., when $g(X)$ is the product of three $g_i(X)$'s. To see how this can be done, let us, for example, consider in Table 4.10 row g_1g_2 corresponding to $g_1(X)\ g_2(X)$ and another row which involves either $g_1(X)$ or $g_2(X)$. Suppose we choose row g_1g_3. From row g_1g_2 we find that 30, 24 and 26 are repeated. But the numbers under 30 in row g_1g_3 are different and the situation is the same with respect to 24 and 26. Also from row g_1g_3 we find that 4 and 28 are repeated. But the number above 4 in row g_1g_2 are different and the situation is the same with respect to 28. This means that the errors not distinguishable by $g_1(X)\ g_2(X)$ are distinguished by $g_1(X)\ g_3(X)$, and the errors not distinguishable by $g_1(X)\ g_3(X)$ are distinguished by $g_1(X)\ g_2(X)$. In other

words the code generated by $g_1(X)\ g_2(X)\ g_3(X)$ can correct all bursts of length 5 or less. Repeating the process for every pertinent combination, we find that the code generated by every $g_i(X)\ g_j(X)\ g_k(X)$ is capable of correcting all bursts of length 5 or less. Also, from the point of view of burst error correction, there is no point in considering products of four or five $g_i(X)$'s. The procedure submitted here is much simpler than an investigation of H^* for each $g_i(X)\ g_j(X)\ g_k(X)$.

It may be interesting to note that the BCH (31, 16) [9, 10, 18] code generated by $g(X) = \text{LCM}\ \{m_1(X), m_3(X), m_5(X)\}$ where $m_i(X)$ is the minimum function of α^i can correct three random errors. If $m_1(X) = g_4(X)$ then $m_3(X) = g_6(X)$ and $m_5(X) = g_1(X)$, i.e., $g(X) = g_1(X)\ g_4(X)\ g_6(X)$. Then this code can correct three random errors or bursts of length 5 or less.

4.4. Example 2. Abramson Codes.

As a second example let us analyse the Abramson code [14] capable of correcting bursts of length 2 or less.

For our $g_1(X)$ let us choose a primitive polynomial of degree, say, q. For the code generated by $g_1(X)$, H_1^* can tell us that a particular single error or double adjacent error has occurred, since each column in H^* are distinct. Clearly, if every code word had even weight, then we can distinguish between these errors. This simply means that $g_1(X)\ (1 + X)$ is the required code. This is, of course, the Abramson code.

As can be easily verified, similar reasoning leads to the Abramson [15] code for bursts of length 3 or less. The code generated by $g(X) = p(X)\ (1 + X + X^2)$ where $p(X)$ is an appropriate primitive polynomial of even degree, say, q. We shall assume that the code exist for a chosen q. If $r(X)$ is a received polynomial, which is the sum of a code word plus a correctable error (burst of length 3 or less), then $r(\alpha)$ gives the set of potential errors, α being a root of $p(X)$. To locate the actual error in this set we may use the parity check matrix H_2^* corresponding to $g_2(X) = 1 + X + X^2$. This is no problem since there are only 4 syndromes to be stored irrespective of the value of q. For this practical case, to each of the four syndromes 00, 01, 11, 10, we attach a set of potential errors to locate the actual error.

Consider the case where $p(X) = 1 + X + X^4$, i.e.,

$$g(X) = (1 + X + X^4)\ (1 + X + X^2),$$
$$= 1 + X^3 + X^4 + X^5 + X^6\ .$$

Then

$$H_2^* = \begin{vmatrix} 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0 \\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 1 \end{vmatrix}.$$

Since $g(X)$ is the generator of the code then it is one of the code word in the code space V, and $v(X) = g(X) = 1 + X^3 + X^4 + X^5 + X^6$. Assuming the error polynomial to be

$$E(X) = X^4 + X^6$$
$$= X^4 (1 + X^2),$$

i.e., a burst error of length 3 in which the middle bit has gone wrong. Then the received polynomial $r(X)$ is given gy

$$r(X) = v(X) + E(X)$$
$$= 1 + X^3 + X^5.$$

Referring to Table 2.1, we find that $r(\alpha) = \alpha^{12}$ and the set of potential errors are:

$e_1(X) = X^0$	$e_2(X) = 1 + X$	$e_3(X) = 1 + X^2$	$e_4(X) = 1 + X + X^2$
α^{12}	$\alpha^8 (1 + \alpha)$	$\alpha^4 (1 + \alpha^2)$	$\alpha^2 (1 + \alpha + \alpha^2)$
13	9	5	3

Next we compute the syndrome $S = \{r(X)\} H^{*T}$

$$S = (1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0) \begin{bmatrix} 0\ 1 \\ 1\ 1 \\ 1\ 0 \\ 0\ 1 \\ 1\ 1 \\ 1\ 0 \\ 0\ 1 \\ 1\ 1 \\ 1\ 0 \\ 0\ 1 \\ 1\ 1 \\ 1\ 0 \\ 0\ 1 \\ 1\ 1 \\ 1\ 0 \end{bmatrix} = (1\ 0)$$

↑ ↑
digits that have gone wrong

For this particular code the set of potential error for each syndrome are as follows: if S = (0 0), then an error pattern e_4 has occurred, For the case where S ≠ (0 0), like in this example, then in Table 4.11, looking in column (1 0), an error pattern e_1 could have started in position 3, 6, 9, 12 or 15; or an error pattern e_2 could have started in position 1, 4, 7, 10 or 13; or an error pattern e_3 could have started in position 2, 5, 8 or 11.

Table 4.11. Possible Error Position

Syndromes / Error Pattern	(0 1)	(1 1)	(1 0)
e_1	1, 4, 7, 10, 13	2, 5, 8, 11, 14	3, 6, 9, 12, 15
e_2	2, 5, 8, 11, 14	3, 6, 9, 12	1, 4, 7, 10, 13
e_3	3, 6, 9, 12	1, 4, 7, 10, 13	2, 5, 8, 11

To get the actual error, $r(\alpha)$ gave us that an error pattern e_1 could have occurred in position 13, or an error pattern e_2 starting in position 9, or an error pattern e_3 in position 5, or an error pattern e_4 in position 3. The only alternative, is an error pattern e_3 starting in position 5. Which is what we expected.

Thus a decoding procedure involving both computation with finite field and parity check can easily be implemented, a fact which does not seem to be too obvious from a consideration of mere H^*.

5. CONCLUDING REMARKS

It was noted in the abstract that an approach based on the consideration of each $g_i(X)$ and $h_i(X)$ would be advantageous. The examples justify this remark. On the other hand as already stated this approach does not produce any startingly new results. In any case it proves useful as illustrated in Example 1, in finding the burst error correcting capability of a code generated by a given $g(X)$.

REFERENCES

1. F. M. Reza, "An Introduction to Information Theory", McGraw-Hill Co., Inc., New York, 1961.

2. W. W. Peterson, "Error Correcting Codes", John Wiley & Son, 1961, p. 3.

3. S. G. S. Shiva and R. Roy, "Some Aspects of Binary Cyclic Codes", Tech. Report No. 68-10, Dept. of Electrical Engineering, University of Ottawa, Ottawa, Canada, June, 1968. To be presented at the Canadian Symposium on Communication in Montreal, November 8th.

4. G. Birkhoff and S. MacLane, "A Survey of Modern Algebra", MacMillan, New York, 1941.

5. W. W. Peterson, "Error Correcting Codes", John Wiley & Son, New York, 1961, p. 98.

6. ———— , op. cit., p. 95.

7. ———— , op. cit., p. 138.

8. R. C. Bose and D. K. Chaudhuri, "On a Class of Error Correcting Binary Group Codes", Information and Control, Vol. 3, 1960, pp. 68-79.

9. R. C. Bose and D. K. Chaudhuri, "Further Results on Error Correcting Binary Group Codes", Information and Control, Vol. 3, 1960, pp. 279-290.

10. A. Hocquenghem, "Code correcteur d'erreurs", Chiffres 2, Sept. 1959, pp. 147-156.

11. R. W. Hamming, "Error Detecting and Error Correcting Codes", Bell Syst. Tech. J., Vol. 29, 1950, pp.147-160.

12. W. W. Peterson, "Encoding and Error Correcting Procedures for the Bose-Chaudhuri Codes", IRE Transaction on Information theory, Sept., 1960.

13. ———— , "Error Correcting Codes", John Wiley & Son, 1961, pp. 169-180.

14. N. W. Abramson, "A Class of Systematic Codes for Non-Independent Errors", IRE Transaction, IT-5, 1959, pp. 150-157.

15. ———— , "Error Correcting Codes from Linear Sequential Networks", presented at the Foutrh London Symposium on Information Theory, Butterworths,London, 1961, pp. 26-38.

16. W. W. Peterson, "Error Correcting Codes", John Wiley & Son, 1961, p. 152.

17. S. W. Golomb, "Shift Register Sequences", Holden-Dary, San Francisco, 1967, p. 62.

18. W. W. Peterson, "Error Correcting Codes", John Wiley & Son, 1961, p. 166, Table 9-1.

VITA

Name: Rémy Roy

Born: Bourlamaque, Québec, Canada,
February 14, 1940.

Educated: Ecole Supérieur Mgr Desmarais,
Val d'Or, Québec.

University: University of Ottawa,
Ottawa, Canada.

Course: Electrical Engineering.

Degree: B.A.Sc. (Ottawa) 1966.