PERMUTATION DECODABLE CYCLIC CODES

A thesis submitted

by

Pui-Wah Yip

to

the School of Graduate Studies of

the University of Ottawa

in partial fulfillment of the requirements

for the degree of

Master of Science

in the subject of

Mathematics

May, 1974

CONTENTS

ACKNOWLEDGEMENT

The author wishes to express her sincere thanks to Professors E.L. Cohen and S.R.S. Shiva for their invaluable advice and constant encouragement in the course of this thesis. Their help allowed her to develop statements and proofs of the Lemmas and Theorems concerning 2 and 3-step permutation decodable cyclic codes.

Thanks are also due to the University of Ottawa for financial help.

ABSTRACT

This thesis is concerned with permutation decoding with binary cyclic codes which have the algebraic structure of ideals over GF(2). We develop bounds on the information rates of 2-error-correcting, 4-error-correcting and 6-error-correcting codes so that these codes are 2-step permutation decodable. We also discuss the case of 3-step permutation decodability of 2-error and 3-error- correcting codes.

INTRODUCTION

In an ideal communication system as shown in figure 1 the symbol that comes out of the channel-symbol-to-sink-symbol converter should match the symbol that entered the source-symbol-to-channel-symbol converter.

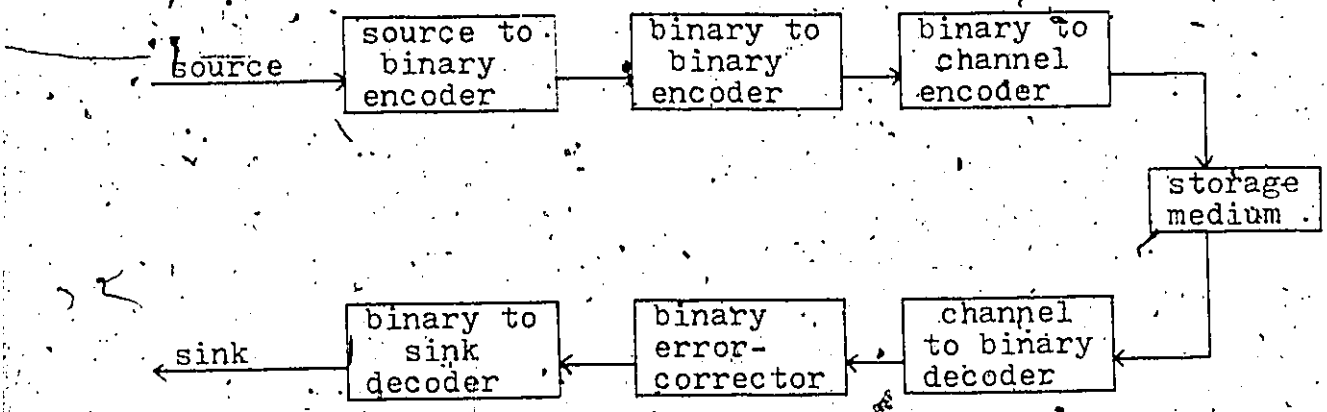


Figure 1

In a practical system there are occasional errors, and it is the purpose of codes to detect such errors. These codes cannot correct every conceivable pattern of errors but rather must be designed to correct only the most likely patterns. Much of coding theory has been based on the assumption that each symbol is affected independently by the noise, so that the probability of a given error pattern depends on the number of errors. Thus, for example, codes have been developed that correct any pattern of t or fewer errors in a block of n symbols.

The codes devised for combatting this kind of error are called random-error-correcting codes.

The encoder for a block code breaks the continuous sequence of information digits into k-symbol blocks. It then operates on these blocks independently according to the particular code to be employed. With each possible information block is associated an n-tuple of channel symbols, where n is greater than k. The n-k digits added to an information block by the encoder are called redundant digits; the ratio $\frac{k}{n}$ is called the code rate. Then the result, called a code word, is transmitted, corrupted by noise, and decoded independently of all other code words. The received n-symbol sequence is called a word and the quantity n is referred to as the block length.

The set of all n-tuples with coordinates chosen from the field of p^m elements, where p is a prime number, is a vector space. A set of these vectors of length n is called a linear code iff it is a subspace of the vector space V^n of n-tuples. Throughout this thesis, n is always assumed to be relatively prime to p and a divisor of p^m-1.

The Hamming metric, or simply the weight, of a vector v, denoted by $|v|$, is defined to be the number of nonzero components. It is known that a linear block code is able to

correct all error patterns of t or fewer errors if the minimum weight (i.e. the minimum distance) of the code is at least 2t+1. This may be restated as follows: If r is a received word in which $\leq$ t errors have occurred, there is a unique code word v at distance $\leq$ t from r. Every other member of the code is at distance $>$ t from r. In Chapter 2, it is assumed that all error patterns are correctable. That is, they are of weight t or less.

Codes discussed here are cyclic codes which are a subclass of linear codes. Cyclic codes can be put into systematic form. That is, the code word consists of the unaltered k-digits information block followed by n-k parity check digits. Three types of results will be presented. First, the basic mathematical properties of cyclic codes are explored in Chapter 1. Then their properties are applied to the permutation decoding in Chapter 2. As nearly all present-day equipment is binary, binary codes are of greatest importance. In Chapter 2, we shall show that some binary cyclic codes with special rates and t even are permutation decodable. Such results are useful in decoding procedures since the existent codes are given, the rates are known. For example, we have found that in the case of double-error-correcting binary cyclic codes with rate $\frac{1}{2} < \frac{k}{n} < \frac{2}{3}$,

2-step permutation decoding will complete the decoding procedure. In particular, for codes with $t = 2$ and rate $\frac{k}{n} = \frac{2b+1}{3b}$, b some positive integer, it will be shown that 2-step permutation decoding with some additional processing will complete the decoding procedure. Also, the Golay code will be shown to be 4-step permutation decodable.

1. PROPERTIES OF CYCLIC CODES

During the past decade, most of the research on block codes has been concentrated on a subclass of linear codes known as cyclic codes. Cyclic codes can be implemented easily for encoding and syndrome calculation. On the other hand, they possess a great deal of algebraic structure and it is possible to find various simple and efficient decoding methods. The basic mathematical properties of cyclic codes are explored in this chapter.

1.1. Ring of polynomials

The ring of polynomials $F[x]$ over a field F has a number of properties which parallel those of the ring I of integers. Moreover, this will be our primary concern here. $F[x]$ may be partitioned by any polynomial $f(x) \in F[x]$ of degree $n \geq 1$ into a ring $F[x]/(f(x)) = \{[a(x)], [b(x)], \ldots\}$ of equivalent classes just as I was partitioned into the ring $I/(m)$. Addition and multiplication are defined as usual and it is easily verified that $F[x]/(f(x))$ is a commutative ring with identity 1 which is the identity of the field F. We call $F[x]/(f(x))$ the ring of polynomials modulo $f(x)$.

The isomorphism $a_i \longleftrightarrow [a_i]$ implies that

$$a_o + a_1 x + \ldots + a_{n-1} x^{n-1} = [a_o] + [a_1][x] + \ldots + [a_{n-1}][x]^{n-1}$$
$$= a_o + a_1 [x] + \ldots + a_{n-1} [x]^{n-1}.$$

As final simplification, let $[x]$ be replaced by η, then we have $F[x]/(f(x)) = \{a_o + a_1\eta + a_2\eta^2 + \ldots + a_{n-1}\eta^{n-1} : a_i \in F\}$. Thus, every residue class equals a polynomial of degree less than n. In fact, $F[x]/(f(x))$ is a commutative linear algebra of dimension n over F since $1, [x], [x]^2, \ldots, [x]^{n-1}$ form a basis.

Let V^n be a vector space of dimension n over F. We may relate V^n and $F(x)/(f(x))$ by the following (1-1) mapping:

$$a_o + a_1 [x] + \ldots + a_{n-1} [x]^{n-1} \longleftrightarrow (a_o, a_1, \ldots, a_{n-1}).$$

The sum of two n-tuples corresponds to the sum of the corresponding polynomials, and multiplication by scalars carries over similarly. In this way, the n-tuples $(a_o, a_1, \ldots, a_{n-1})$ and the polynomial $a_o + a_1\eta + \ldots + a_{n-1}\eta^{n-1}$ will be considered different ways of representing the same element of $F[x]/(f(x))$. An element of it will sometimes be called a vector, sometimes a polynomial.

1.2 Cyclic codes and Galoi's Fields

Let R_n be the ring of polynomials modulo $x^n - 1$. If V is

an ideal of R_n, then $g \in V$ implies $rg \in V$ for any $r \in R_n$. In particular, $rg \in V$, $r^2g \in V$, ... Thus an ideal in R_n corresponds one-to-one to a subspace V' of V^n which is invariant under a cyclic permutation of coordinates.

In view of this, we call a subspace V of V^n a cyclic code if for each vector $u = (a_0, a_1, \ldots, a_{n-1}) \in V$ of V^n, the vector $u^1 = (a_{n-1}, a_0, a_1, \ldots, a_{n-2})$ obtained by shifting the components of u cyclically one unit to the right is also in V. The n-tuples will be considered to be the elements of R_n. Given a polynomial a(x) of degree greater than n, the polynomial of smallest degree in the same equivalent class is found by dividing a(x) by x^n-1. The remainder is a polynomial of degree less than n and corresponds to a residue class of R_n and hence a vector in V. Since a cyclic code in V^n corresponds to an ideal in R_n and vice versa, we represent both ideal and cyclic code by the same symbol V.

Lemma 1. An ideal V in R_n consists of all multiples of a polynomial g(x) which divides x^n-1 in F[x]. g(x) is the unique polynomial of minimal degree in V. [7; p.151-152]

A cyclic code is therefore completely specified by g(x).

The polynomial $g(x)$ is called the generator of the ideal, or equivalently, the generator of the cyclic code V. The polynomial $h(x) = (x^n-1)/g(x)$ will be called the parity check polynomial (or reciprocal factor) of the code V. If the degree of $h(x)$ is k, then the dimension of the code V as a vector space of V^n is k and $g(x)$ has degree n-k. [7;p.153]

The element $[f(x)]$ is in the code V iff $f(x)$ is divisible by $g(x)$. Since $h(x)$ divides x^n-1, it can be used as the generator of a cyclic code. Such a code and its code words are characterized by THEOREM 1. A polynomial $r(\eta)$ will be said to be in the null space of an ideal J in R_n if $r(\eta)s(\eta) = 0$ for any $s(\eta)$ in J.

THEOREM 1. $[f(x)]$ is in the null space of the ideal V generated by $h(x)$ iff $[f(x)]$ is in the ideal V generated by $g(x)$. [7;p.154]

The code V' generated by $h(x)$ is called the dual code of V. If V^n is over a field F with p elements, the code V has p^k code words and its dual code has p^{n-k} code words. Many properties of the code V can be given from its dual codes. For example, the weight distribution (i.e. the number of A_i for $i=0,1,\ldots,n$; where A_i is the number of code words of weight i)

of the code V can be calculated from that of its dual code. [7;p.64]

Suppose K is a finite field. Since the prime field of a field of characteristic zero has infinitely many elements, K must be of prime characteristic, say Char = p. If the prime field of K is denoted by GF(p), K can be thought of as a vector space over GF(p). Suppose $[K:GF(p)] = m$, (the dimension of K over GF(p)), then K has p^m elements. We denote a field having p^m elements by $GF(p^m)$. These fields are called Galois fields. The elements of $GF(p^m)$ are the roots of the polynomial $x^{p^m}-x$ and $GF(p^m)$ is the splitting field of $x^{p^m}-x$ over GF(p). Hereafter all polynomials are assumed to have coefficients in GF(p) unless otherwise specified.

THEOREM 2. The polynomial x^m-1 divides x^s-1 iff $m|s$. [7;p.157-158]

($m|s$ means m divides s)

THEOREM 3. For any positive integers s and m,

$m|s$ iff $GF(p^m)$ is a subfield of $GF(p^s)$. [6;p.257]

Lemma 2. If α in $GF(p^m)$ is a root of an irreducible polynomial f(x) of degree s, then all its roots are given by α^p, α^{p^2}, ..., $\alpha^{p^{s-1}}$ and have the same order. [7;p.160-161]

THEOREM 4. Every irreducible factor of $x^{p^m}-x$ has degree which divides m. Conversely, an irreducible polynomial of degree s over GF(p) with s dividing m is a factor of $x^{p^m}-x$.

Proof: Let f(x) be an irreducible factor of $x^{p^m}-x$ of degree s; and α be a root of f(x). All the conjugates of α are $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^{s-1}}$ by Lemma 2 and hence GF(p)(α) contains all roots of f(x). It is clear ~~that~~ GF(p)(α) is a subfield of $GF(p^m)$ with p^s elements. Therefore, by THEOREM 3, $s \mid m$.

Conversely, if f(x) is an irreducible polynomial of degree s over GF(p) and s divides m, then by THEOREM 3 again, $GF(p^s) \subseteq GF(p^m)$. Hence all roots of f(x) are contained in $GF(p^m)$ and therefore f(x) divides $x^{p^m}-x$.

Q.E.D.

By an h-th root of unity over GF(p) we shall mean a root of the polynomial x^h-1 in any extension field. If the order of a root of unity is exactly h, it will be called a primitive h-th root of unity. A polynomial over GF(p) with a primitive h-th root of unity as a root is called a primitive polynomial.

Let α be a primitive h-th root of unity. Since the powers of α include all h-th roots of unity, we have the following factorization: $x^h-1 = \prod_{i=0}^{h-1}(x-\alpha^i) = \prod_{i=1}^{h}(x-\alpha^i)$. If $h = sd$, then $\alpha^s, \alpha^{2s}, \ldots, \alpha^{ds}$ are all roots of the equation $x^d-1 = 0$. This equation has degree d, so it can have no more than d roots in any field. Therefore, if α has order h, and d divides h, the powers of α include all d-th roots of unity. Furthermore, every field element whose order divides h is a power of α. This suggests that we can partition the powers of α according to their orders:

$x^h-1 = \prod_{d|h}\prod_{\beta}(x-\beta)$, where β is a field element of order d.

If $Q_d(x)$ is a polynomial whose roots are the field elements of order d, then $x^h-1 = \prod_{d|h} Q_d(x)$ and $Q_d(x)$ is called the cyclotomic polynomial. The formula $x^h-1 = \prod_{d|h} Q_d(x)$ determines $Q_h(x)$ uniquely. For if $Q_d(x)$ is known for all positive $d < h$, $Q_h(x)$ can be determined by division. It is known that the cyclotomic polynomials are given by $Q_h(x) = \prod_{d|h}(x^d-1)^{\mu(h/d)}$ where $\mu(.)$ is the " Mobius Function " which is defined as follows:

$$\mu(r) = \begin{cases} 0 & \text{if } p_i^2 | r \text{ for any } p_i \\ (-1)^\lambda & \text{if } r = p_1 \ldots p_\lambda \\ 1 & \text{if } r = 1 \end{cases}$$

($p_1 p_2 \ldots p_\lambda$ are various prime factors of the number r)

Let n be relatively prime to p and a divisor of p^m-1. From THEOREM 3, we know that x^n-1 divides $x^{p^m-1}-1$. Thus x^n-1 can be factored into distinct linear factors and all irreducible factors of x^n-1 are distinct. When n is not too large, the cyclotomic polynomials and what we have proved may help to find out all irreducible polynomials of x^n-1. The factorization of x^n-1 into distinct irreducible polynomials plays an important role for a cyclic code of block length n and it will be discussed later.

The least common multiple of the orders of the roots of a polynomial p(x) is called the exponent of p(x). If the exponent of p(x) is e, then p(x) divides x^e-1 and e divides n.

Lemma 3. Suppose the exponent of the generator g(x) of the code V is e. If $e < n$, then code V is of minimum weight 2.

Proof: If the exponent of g(x) is e, then g(x) divides x^e-1. By Lemma 1, x^e-1 is a code word of V and thus the code V is of minimum weight 2. No code word is of weight 1 for otherwise we shall have a polynomial of degree less than that of g(x) by the cyclic property of V.

Q.E.D.

By the Galois group of K over F, we mean the group of all

automorphisms of K that leave every element of F fixed. If $p(x)$ is a polynomial with coefficients in F, we can define the Galois group of a splitting field of $p(x)$ over F. Suppose $p(x)$ is a polynomial of degree n with simple roots. If K is a splitting field of $p(x)$, we may write

$$p(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \quad \text{and}$$

$$K = F(\alpha_1, \alpha_2, \ldots, \alpha_n), \text{ where } \alpha_i \in K.$$

An automorphism σ of the splitting field effects a certain permutation of the roots $\sigma(\alpha_i) = \alpha_{\lambda_i}$. We shall denote the roots by their subscripts alone and σ will then be defined by the notation $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \end{pmatrix}$. If the group permutes r of the indices in a transitive way, say 1 is carried over into the indices $1,2,\ldots,r$, the set of indices $1,2,\ldots,r$ is called a cycle (an orbit). We may divide all the indices into cycles, a chain of transitivity consists of all the indices that can be carried into each other by the permutations of the group.

THEOREM 5. There is a one-to-one correspondence between the irreducible factors of a separable polynomial $p(x)$ over F and the cycles of its Galois group.

Proof: Let $p_1(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_r)$ be an irreducible factor of $p(x)$ over F. From $p_1(\alpha_1) = 0$ we have $p_1(\sigma(\alpha_1)) = 0$ where σ is any element of the Galois-group of $p(x)$. Consequently, $\sigma(\alpha_1)$ is one of the $\alpha_1, \alpha_2, \ldots, \alpha_r$. Furthermore, α_1 has at least r distinct images for otherwise it would satisfy an equation of lower degree. It follows that each α_i, $i \leq r$, is an image of α_1 in some automorphism, and α_1 has no other images. In other words, the irreducible factor $p_1(x)$ determines the cycle $1,2,\ldots,r$.

Q.E.D.

Corollary 5.1. The number of irreducible factors of x^n-1 over GF(p) is the number of cycles of its Galois group.

Corollary 5.2. Let m_i be the degree of an irreducible separable polynomial $p_i(x)$ over GF(p). Then m_i is the length of the corresponding cycle.

THEOREM 6. If the number of cycles of the Galois group of x^n-1 is d, then there are $\sum_{1}^{d-1} \binom{d}{i}$ cyclic codes of block length n.

Proof: If the number of cycles of G is d, then x^n-1 has d distinct irreducible factors. Combining these d distinct irreducible factors by multiplication, we have $\binom{d}{1} + \binom{d}{2} + \ldots + \binom{d}{d-1} = \sum_{1}^{d-1} \binom{d}{i}$ different factors of x^n-1. Hence there are $\sum_{i=1}^{d-1} \binom{d}{i}$ cyclic codes of block length n.

Q.E.D.

1.3 Specification of a cyclic code by the roots of its generator

Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be the elements of $GF(p^m)$ such that they are roots of a polynomial f(x). It is known that for each α_i, there is a unique monic irreducible polynomial $p_i(x)$ of least degree such that $p_i(\alpha_i) = 0$. ($p_i(x)$ is often called a minimum polynomial of α_i) and f(x) is divisible by $p_1(x) \ldots p_r(x)$. Hence it is divisible by L.C.M. ($p_1(x), p_2(x), \ldots, p_r(x)$). Let g(x) = L.C.M. ($p_1(x), p_2(x), \ldots, p_r(x)$). The exponent of g(x) is e = L.C.M. ($e_1, e_2, \ldots, e_r$), where e_i is the exponent of $p_i(x)$. If $e = p^m-1$, then g(x) divides $x^{p^m-1}-1$ and hence g(x) generates a cyclic code V of block length $n = p^m-1$. The code V has minimum weight at least 2. If $e < p^m-1$, then g(x) generates a cyclic code V of block length n with

n a multiple of e and a divisor of p^m-1. Thus the statement that $[f(x)]$ is in a code V iff $\alpha_1, \alpha_2, \ldots, \alpha_r$ are roots of $f(x)$ uniquely specifies a cyclic code.

If it is specified that $f(x)$ must have α_i as a root of multiplicity r_i, then the minimum polynomial $p_i(x)$ of α_i must appear in $g(x)$ repeated r_i times. If $n' = p^s n_o$, where n_o and p are relatively prime, then $x^{n'}-1 = (x^{n_o}-1)^{p^s}$. Thus $x^{n'}-1$ always has all its roots repeated the same number of p^s times. The value of n' can be found for repeated roots as follows: Take n_o to be the least common multiple of the orders of the elements $\alpha_1, \alpha_2, \ldots, \alpha_r$. Each is a single root of $x^{n_o}-1$. Let r_m be the maximum multiplicity of any root, and s the smallest integer such that $r_m \leq p^s$. Then $n' = n_o p^s$.

Example 1. Let p = 2 and let α be a primitive element of $GF(2^4)$. Then $\alpha^{15} = 1$. Consider a code for which a vector $f(x)$ is a code word iff $\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5$, and α^6 are roots. Let $p_i(x)$ denote the minimum polynomial of α^i. Then $\alpha, \alpha^2, \alpha^4, \alpha^8$ are the roots of $p_1(x)$, and $p_1(x) = p_2(x) = p_4(x) = p_8(x)$. Similarly, $\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24} = \alpha^9$ are the roots of $p_3(x)$. Then $g(x)$ is $p_1(x)p_3(x)p_5(x)$ and so $g(x)$ has degree 10. The code generated by $g(x)$ is called a primitive BCH code with n = 15, k = 5, t = 3.

Example 2. Let α be the cube of a primitive element of $GF(2^6)$. Then α has order 21. If the minimum polynomial of α^j is denoted by $p_j(x)$, then $\alpha^{21} = 1$, and α, α^2, α^4, α^8, α^{16}, $\alpha^{32} = \alpha^{11}$ are roots of $p_1(x)$; α^3, α^6, α^{12} are roots of $p_3(x)$. Therefore, $g(x) = p_1(x)p_3(x)$ has roots α, α^2, α^3, α^4 and has degree 9. The code generated by $g(x)$ is called a nonprimitive BCH code that corrects all double errors. It has $n = 21$, $k = 12$ as parameters.

1.4 Representation of a cyclic code as a direct sum of its minimal ideals

A commutative ring is said to satisfy the descending chain condition DCC of ideals if whenever $I_1 \supseteq I_2 \ldots \supseteq I_N \ldots$ is a descending chain of ideals, there exists an integer such $I_L = I_N$, for $L \geq N$. Clearly, R_n has this property.

An ideal I of R_n is called a minimal ideal if (i) $I \neq (0)$ and (ii) whenever $I \supseteq J \supseteq (0)$, J an ideal of R_n, then either $J = I$ or $J = (0)$.

Lemma 4. Let $I \neq (0)$ be an ideal of R_n generated by $I(x)$ with reciprocal factor $f(x)$. I is a minimal ideal iff $f(x)$ is irreducible.

Proof: (i) Suppose $f(x)$ is reducible, say $f(x) = f_1(x)f_2(x)$. The ideal J generated by $I(x)f_1(x)$ is clearly a proper subideal of I and $J \neq (0)$. Then I is not a minimal ideal.

(ii) Let $J \neq (0)$ be a proper subideal of I. Let $g_1(x)$ and $g_2(x)$ be the generator polynomial and reciprocal factor of J respectively. Since every element in J is a multiple of $I(x)$, we have $g_1(x) = I(x)g'(x)$. for some $g'(x)$. Hence $I(x)g'(x)g_2(x) = x^n-1$ and therefore $f(x) = g'(x)g_2(x)$.

That is, $f(x)$ is reducible.

Q.E.D.

An ideal M of R_n is called a maximal ideal if (i) $M \subset R_n$ and (ii) whenever N is an ideal of R_n such that $M \subseteq N \subseteq R_n$, then either $N = M$ or $N = R_n$.

Lemma 5. Let M be an ideal of R_n generated by $m(x)$ with reciprocal factor $f(x)$. M is maximal iff $m(x)$ is irreducible.

Proof: (i) Assume $m(x)$ is irreducible. We shall show that $R_n/([m(x)])$ is a field. Let $[a(x)] \neq 0 \in R_n$ such that

$[a(x)]+([m(x)]) \neq 0+([m(x)])$. Then $[a(x)] \notin ([m(x)])$. Since $m(x)$ is irreducible, $a(x)$ and $m(x)$ are relatively prime; thus there exist $[u(x)], [v(x)] \in R_n$ such that $a(x)u(x)+m(x)v(x) = 1$. So we have $a(x)u(x) \equiv 1 \bmod m(x)$. That is,

$$\{[a(x)]+([m(x)])\}\{[u(x)]+([m(x)])\} = 1+([m(x)]).$$

This shows that $R_n/([m(x)])$ is a field and hence $([m(x)])$ is maximal.

(ii) Assume $([m(x)])$ is maximal.

Suppose $m(x)$ is reducible; say $m(x) = m_1(x)m_2(x)$. Since the degree of $m_1(x)$ and $m_2(x)$ respectively are less than the degree of $m(x)$, $m(x) \nmid m_1(x)$ and $m(x) \nmid m_2(x)$. ($m(x) \nmid m_1(x)$ means $m(x)$ does not divide $m_1(x)$) Hence $[m_1(x)] \notin ([m(x)])$ and $[m_2(x)] \notin ([m(x)])$. That is, $[m_1(x)]+([m(x)]) \neq 0+([m(x)])$ and

$$[m_2(x)]+([m(x)]) \neq 0+([m(x)]).$$

But $[m_1(x)m_2(x)]+([m(x)]) = 0+([m(x)])$. Thus $R_n/([m(x)])$ is not a field and therefore $([m(x)])$ is not maximal. This contradiction shows that $m(x)$ is irreducible.

Q.E.D.

The above two lemmas are helpful in choosing the generator polynomial $g(x)$ of a cyclic code. For example, if the reciprocal factor $p(x)$ is a primitive polynomial, then $g(x)$ generates a minimal ideal V which has p^m code words. Such a code is called a maximum length code. It can be shown that the code V consists of the all-zero code word and p^m-1 code words of the same weight, p^{m-1}. [7;p.222-223]

It is not hard to show that R_n is a semi-simple ring and hence every minimal ideal I of R_n has an idempotent $e \neq 0 \in I$ such that $I = R_n \cdot e$. The following theorem suggests a way to find an idempotent of each minimal ideal I. For notation simplicity, we shall denote a polynomial $A(x)$ of degree $\leq n-1$ and its equivalent class $[A(x)]$ by the same symbol $A(x)$. Thus, whenever we say $A(x) \in R_n$, we mean $[A(x)]$ is in R_n.

THEOREM 7. Every ideal V of R_n contains a unique polynomial $E(x)$ with the following properties:

(i) $E(x) \equiv E^2(x) \bmod x^n-1$; $E(x)$ is called a primitive idempotent of V.

(ii) $V = R_n \cdot E(x)$; $E(x)$ generates V.

(iii) $E(x)$ is a unit for V.

(iv) $\sigma(E(x))$ is an idempotent of $\sigma(V)$; where σ is an automorphism of R_n.

Proof: Let $g(x)$ and $h(x)$ be the generator polynomial and reciprocal factor of V respectively. Since n and p are relatively prime, there exist polynomials $h_1(x)$, $h_2(x)$ such that $h_1(x)g(x)+h_2(x)h(x) = 1$ and $h_1(x)$, $h_2(x)$ are relatively prime to $h(x)$, $g(x)$ respectively.

(i) Let $E(x) = h_1(x)g(x)$, then

$$E(x) = E^2(x)+E(x)h_2(x)h(x)$$
$$= E^2(x)+h_1(x)g(x)h_2(x)h(x)$$
$$= E^2(x)+h_1(x)h_2(x)(x^n-1).$$

Hence $E(x) \equiv E^2(x) \bmod x^n-1$.

Thus $E(x)$ is an idempotent of V.

(ii) Since the generator polynomial of $R_n \cdot E(x)$ is the highest common factor of $E(x)$ and x^n-1, this is $g(x)$ by construction of $E(x)$.

Hence $V = R_n \cdot E(x)$.

(iii) If $b(x) \in V$, then $b(x) = b'(x)E(x)$ and

$$b(x)E(x) = b'(x)E^2(x)$$

But $b'(x)E^2(x) \equiv b'(x)E(x) \bmod x^n-1$;

so $b(x)E(x) = b(x)$.

$E(x)$ is an identity of V and hence $E(x)$ is unique.

(iv) $\sigma(E(x)) \equiv \sigma(E^2(x)) \bmod x^n-1$ and

$\sigma(E^2(x)) \equiv \sigma(E(x))\sigma(E(x)) \bmod x^n-1$.

Thus $\sigma(E(x))$ is an idempotent of $\sigma(V)$.

Q.E.D.

Lemma 6. Let e be a nonzero idempotent in a semi-simple ring R.

Let $R_1 = \{a-ae : a \in R\}$. Then

(i) $R = R_1 \oplus R \cdot e$

(ii) If $R_1 \neq (0)$, there exists a minimal ideal $R \cdot f$ of R contained in R_1 and $ef = fe = 0$, $f^2 = f \neq 0$.

(iii) e+f is an idempotent. [6; p. 288]

THEOREM 8. Suppose x^n-1 has r irreducible factors: $f_1(x), \ldots, f_r(x)$.

Let I_i be the minimal ideal of R_n with reciprocal factor $f_i(x)$. Then

(i) $R_n = I_1 \oplus I_2 \oplus \ldots \oplus I_r = R_n \cdot (E_1(x)+E_2(x)+\ldots+E_r(x))$

(ii) $\sum_1^r E_i(x) = 1$

($E_i(x)$ is the primitive idempotent of I_i)

Proof: Let $I_1 = R_n \cdot E_1(x)$ be a minimal ideal generated by $E_1(x)$ with $f_1(x)$ as reciprocal factor. By Lemma 6, $R_n = V_1 \oplus R_n \cdot E_1(x)$, where $V_1 = \{a(x)(1-E_1(x)) : a(x) \in R_n\}$. Clearly, V_1 is an ideal with generator polynomial $f_1(x)$, reciprocal factor $f_2(x) \ldots f_r(x)$ and primitive idempotent $1-E_1(x)$. By application of Lemma 6 again, let $I_2 = R_n \cdot E_2(x)$ be a minimal ideal of R_n contained in V_1 with reciprocal factor $f_2(x)$. Then

$R_n = V_2 \oplus R_n \cdot E_2(x) \oplus R_n \cdot E_1(x)$;

where $V_2 = \{a(x)(1-E_2(x)) : a(x) \in R_n\}$ with generator polynomial $f_1(x)f_2(x)$.

$E_1(x)E_2(x) \equiv E_2(x)E_1(x) \equiv 0 \bmod x^n-1$ and

$E_2(x) \equiv E_2^2(x) \bmod x^n-1$, $E_2(x) \in V_1$. Also, if

$b(x) \in R_n \cdot E_2(x) \oplus R_n \cdot E_1(x)$, then $b(x) = a_2(x)E_2(x)+a_1(x)E_1(x)$

and $(E_2(x)+E_1(x))b(x) = (E_2(x)+E_1(x))(a_2(x)E_2(x)+a_1(x)E_1(x))$.

$= a_2(x)E_2(x)+a_1(x)E_1(x)$.

$\therefore R_n \cdot E_2(x) \oplus R_n \cdot E_1(x) = R_n \cdot (E_2(x)+E_1(x))$. In addition, if $b(x) \in V_1$, then $b(x)$ has $f_1(x)$ as a factor, hence $b(x)E_1(x) \equiv 0 \bmod x^n-1$; so we have

$V_2 = \{a(x)[1-(E_1(x)+E_2(x))] : a(x) \in R_n\}$.

Thus $R_n = V_2 \oplus R_n \cdot E_2(x) \oplus R_n \cdot E_1(x) = V_2 \oplus R_n \cdot (E_2(x)+E_1(x))$.

By repeated application of Lemma 6, and by the fact

that $V_1 \supset V_2 \supset \ldots \supset V_{r-1} \supset V_r = (0)$, we get

$R_n = I_1 \oplus I_2 \oplus \ldots \oplus I_r = R_n \cdot (E_1(x)+E_2(x)+\ldots+E_r(x))$,

$E_i(x)E_j(x) \equiv 0 \bmod x^n-1$ for $i \neq j$ and

$E_i(x) \equiv E_i^2(x) \bmod x^n - 1$.

It is easily seen that $\sum_1^r E_i(x) = 1$.

Q.E.D.

Corollary 8.1 Any ideal V in R_n is the direct sum of all minimal ideals contained in V. The primitive idempotent of V is the sum of primitive idempotent of each minimal ideal contained in V.

THEOREM 8 gives a method of partitioning a cyclic code V into disjoint sets. Let g(x) and h(x) be the generator and reciprocal factor of V respectively. Let $h(x) = h_1(x)h_2(x)\ldots h_r(x)$, where $h_i(x)$ is irreducible factor of h(x) and has degree m_i, exponent e_i. From THEOREM 8, we get a descending chain $V_o = V \supset V_1 \supset V_2 \supset \ldots \supset V_{r-1} \supset V_r = (0)$; where V_i is generated by $g(x)h_1(x)h_2(x)\ldots h_i(x)$; $i \leq r$. Define $V_{i-1}-V_i$ to mean the set of all code words that are in V_{i-1} but not in V_i. It is seen that the collection V_o-V_1, V_1-V_2, ..., $V_{r-1}-V_r$ partitions the code V. All the code words in $V_{i-1}-V_i$ have the same form

$f(x)g(x)h_1(x)h_2(x) \ldots h_{i-1}(x)$, where $f(x)$ is not divisible by $h_i(x)$.

A cyclic class consists of those code words which are cyclic shifts of one another; the size of the class is called its period. Let b be the smallest integer such that $x^b f(x)g(x) \equiv f(x)g(x) \bmod x^n-1$; then we have $(x^b-1)f(x)g(x) \equiv 0 \bmod x^n-1$. This shows that $h(x)$ divides $(x^b-1)f(x)$ and $f(x)g(x)$ represents a cycle of length b. Similarly, the periods of the cycles of V_i can be determined. Let d be the smallest integer such that $x^d f(x)g(x)h_1(x)\ldots h_i(x)$

$$\equiv f(x)g(x)h_1(x)\ldots h_i(x) \bmod x^n-1.$$

We have $(x^d-1)f(x)g(x)h_1(x)\ldots h_i(x) \equiv 0 \bmod x^n-1$. That is, $h_{i+1}(x)\ldots h_r(x)$ divides $(x^d-1)f(x)$. Thus $f(x)g(x)h_1(x)\ldots h_i(x)$ represents a cycle of length d.

Let E(x) be the primitive idempotent of code V. We know that $E(x) = E_1(x)+E_2(x)+\ldots+E_r(x)$ and $V = I_1 \oplus I_2 \oplus \ldots \oplus I_r$; where $E_i(x)$ is the primitive idempotent of I_i which has $h_i(x)$ as a reciprocal factor. Hence each I_i has p^{m_i} code words. From the above discussion, we can see that the period of the cycles of each minimal ideal I_i of the code V is the exponent e_i of $h_i(x)$. Since there are $p^{m_i}-1$ nonzero code words in I_i, there are $c_i = p^{m_i}-1/e_i$ cycle representatives in it.

It is obvious that all the code words in a cycle have the same weight. If we can determine a representative and the period of each cyclic class, we have a great deal of information about the code. For example, the weight distribution is completely determined. The weight distribution has a number of applications in the study of codes. For instance, the probability of an undetectable error for a linear code used strictly for error detection can be calculated. [2;p.397-400], [4], [7;p.64].

To view a cyclic code V as the direct sum of its minimal ideals, we can obtain methods to determine a cycle representative. [1], [9]. It is not necessary to determine all the cycle representatives if one applies permutations which map one cycle representative into another. The permutation σ: $w \longrightarrow wp \pmod n$ corresponds to an automorphism τ: $x^w \longrightarrow x^{wp} \pmod{x^n-1}$ of R_n. Every ideal V of R_n is preserved by τ. Thus if we raise any code word to the power of p, we can get another code word (possibly the same) of the same weight. By using this property, some results on permutation decodable cyclic codes are obtained in Chapter 2.

2. PERMUTATION DECODING FOR CYCLIC CODES

A symmetry of a systematic code is a permutation of bit positions in each code word which preserves the code as a whole. Permutation Decoding makes use of these symmetries to build up a decoding algorithm for the code. From the algebraic structure of a cyclic code which we discussed in Chapter 1, the problem to find a set of symmetries for a cyclic code is somewhat easier. For some special cyclic codes, the problem is solved in this Chapter.

Permutation Decoding for cylcic codes is most effective for decoding single-error-correcting codes. It becomes easier as the redundancy of the code increases. Hereafter, we shall discuss Permutation Decoding for cyclic codes only.

We assume that we wish to decode an (n, k, t) cyclic code V of V^n described in Chapter 1 with generator polynomial g(x) of degree n-k.

The coordinate places in V^n are labeled by the number 0, 1, ..., n-1. If w stands for one of these numbers, the cyclic permutation is $T: w \longrightarrow w+1$ (addition mod n). The powers of the cyclic permutation are $T^2: w \longrightarrow w+2, \ldots, T^{n-1}: w \longrightarrow w+n-1, I = T^n: w \longrightarrow w+n = w$.

Thus a cyclic code in V^n is a code which is invariant under T and hence invariant under T^2, T^3, ..., T^{n-1}. Corresponding to the cyclic permutation T, the mapping $\rho: x^i \longrightarrow x^{i+1} \pmod{x^n-1}$ is an automorphism of R_n. Clearly, every cyclic code is preserved by ρ. Thus, if a word $R(x) \in R_n$, then $(x^iR(x) \bmod x^n-1) \in R_n$ and we call $x^iR(x) \bmod x^n-1$ the i-th cyclic shift of R(x). In particular, if a code word $v(x) \in V$, then $(x^iv(x) \bmod x^n-1) \in V$. We know that if $v(x) \in V$, then $(x^iv^{p^j}(x) \bmod x^n-1) \in V$.

2.1 Permutation decodable codes

Let $V(x) \in V$ be the transmitted code word and let R(x) be the received word. Then the error pattern caused by the channel disturbance is $E(x) = R(x)-V(x)$, where E(x) is of weight t or less. Dividing R(x) by g(x), we have $R(x) = q(x)g(x)+S(x)$, where S(x) is a polynomial of degree $\leq n-k-1$ and is called the syndrome of the received word R(x). If the syndrome is zero, then R(x) is divisible by g(x). By [Lemma 2, Chapter 1] R(x) is a code word of V and the decoder will take R(x) as the transmitted code word. If the syndrome is nonzero, the received word is not a code word and errors have been detected.

Lemma 7. The syndrome of $R(x)$ is equal to the remainder resulting from dividing the error pattern $E(x)$ by $g(x)$.

Proof: Let $V(x) \in V$ be the transmitted code word.

We have $R(x) = V(x)+E(x)$. Dividing $R(x)$ by $g(x)$, we have $R(x) = q(x)g(x)+S(x)$.

Hence $R(x) = q(x)g(x)+S(x) = A(x)g(x)+E(x)$ for some $A(x)$ such that $V(x) = A(x)g(x)$.

That is, $E(x)-S(x) = (q(x)-A(x))g(x)$.

$E(x) \bmod g(x) \equiv S(x)$.

Q.E.D.

Corollary L.7.1 The syndrome of $(R^{p^i}(x) \bmod x^n-1)$ is equal to the remainder resulting from dividing $(E^{p^i}(x) \bmod x^n-1)$ by $g(x)$.

Lemma 8. The syndrome of $(x^iR(x) \bmod x^n-1)$ is equal to $(x^iS(x) \bmod x^n-1) \bmod g(x)$; where $S(x) \equiv R(x) \bmod g(x)$.

Proof: Let $R(x) = q(x)g(x)+S(x)$ and $x^iR(x) \bmod x^n-1 \equiv A(x)g(x)+t(x)$.

Then we have $\left[x^iq(x)g(x)+x^iS(x)\right] \bmod x^n-1 \equiv A(x)g(x)+t(x)$.

That is, $(x^iq(x)g(x) \bmod x^n-1)+x^iS(x) \bmod x^n-1$

$\equiv A(x)g(x)+t(x)$, or

$\left(x^iq(x)g(x)-A(x)g(x)\right) \bmod x^n-1 \equiv t(x)-(x^iS(x) \bmod x^n-1)$.

Since $x^i q(x)g(x)-A(x)g(x)$ is divisible by $g(x)$,

$$t(x) \bmod g(x) \equiv t(x) \equiv (x^i S(x) \bmod x^n-1) \bmod g(x).$$

Q.E.D.

Corollary L.8.1 The syndrome of $(R^{p^i}(x) \bmod x^n-1)$ is equal to

$$(x^{p^i} S(x) \bmod x^n-1) \bmod g(x).$$

Lemma 9. Let $S(x) \equiv R(x) \bmod g(x)$ and $R(x) = V(x)+E(x)$.

Then $|S(x)| \leq t$ iff $E(x)$ is of degree $\leq n-k-1$.

Proof: If $E(x)$ is of degree $\leq n-k-1$, then by Lemma 7, $E(x) = S(x)$ and hence $|S(x)| \leq t$.

Now assume $|S(x)| \leq t$. Since $E(x) = B(x)g(x)+S(x)$ for some $B(x)$, $E(x)-S(x)$ is a code word of V and therefore $|E(x)-S(x)| \geq 2t+1$. This is impossible since $|E(x)-S(x)| < |E(x)|+|S(x)| < 2t$.

Thus the fact that $E(x) - S(x)$ is a code word implies that $E(x) - S(x)$ is the all zero word; so $E(x) = S(x)$ and $E(x)$ is of degree $\leq n-k-1$.

Q.E.D.

From Lemma 9, we see that if the errors in $R(x)$ are confined to the n-k parity check positions or if the syndrome

of R(x) is of weight t or less, then the syndrome is identical to the error pattern S(x) = E(x). Thus, correction can be accomplished simply by subtracting the syndrome from the n-k received parity check digits. Since we know that every cyclic code is a systematic code, the first k digits are error free provided E(x) is of degree $\leq n-k-1$.

Suppose that the errors are not confined to the n-k parity check positions of R(x) but are confined to n-k consecutive positions (including the end round case), say $x^i, x^{i+1}, \ldots, x^{n-k+i-1}$. After n-i cyclic shifts of R(x), the error will be shifted to the n-k parity check positions of the cyclically shifted received word $x^{n-i}R(x)$. Then the syndrome of $x^{n-i}R(x)$ will give information to the errors confined to the positions $x^i, x^{i+1}, \ldots, x^{n-k+i-1}$ of R(x). As a result, the errors can be corrected. Permutation Decoding for cyclic code is based on these facts.

DEFINITIONS: Let R(x) be any received word and let

$$S_{ij}(x) \equiv (x^j R^{p^i}(x) \bmod x^n-1) \bmod g(x).$$

If $|S_{ij}(x)| \leq t$ for some i and j, then code V is said to be Permutation Decodable (in brief P.D.) and $(x^{-j}S_{ij}(x) \bmod x^n-1)^{p^{-i}}$ is the error pattern. If the maximum value of i required is s-1 for all

possible error patterns E(x) with weight $\leq t$, then code V is said to be s-step P.D.

2.2 1-step permutation decodable codes

THEOREM 9. Code V is 1-step P.D. iff $\frac{k}{n} < \frac{1}{t}$. [4]

Proof: Assume code V is 1-step P.D.

Then every n-symbol error pattern E(x) with weight t or less will contain a sequence of at least k successive zeros. Hence $n > tk$ or $\frac{k}{n} < \frac{1}{t}$.

Assume $\frac{k}{n} < \frac{1}{t}$. Suppose code V is not 1-step P.D.

Then there exists at least one error pattern E(x) of weight t which does not contain a sequence of k zeros; or equivalently, does not have a gap of length $\geq k$. Since the code is cyclic, it is enough if we consider E(x) of the following type:

$$E(x) = b_0 + b_1 x^{a_1} + b_2 x^{a_2} + \ldots + b_{t-1} x^{a_{t-1}}; \quad b_i \in GF(p).$$

Since there is no gap of length $\geq k$ in E(x), E(x) must satisfy the following condition:

$$a_{i+1} - a_i \leq k \text{ and } n - a_{t-1} \leq k \text{ for } i = 0, 1, \ldots, t-2, \; a_0 = 0.$$

This condition will give $n \leq tk$ or $\frac{k}{n} \geq \frac{1}{t}$.

This contradicts the assumption.

$\therefore$ code V is 1-step P.D. Q.E.D.

If code V is a binary code and is 1-step P.D., then the calculation of the syndrome of $(x^iR(x) \bmod x^n-1)$ is greatly simplified. This is because of the application of Lemma 8 and of the properties of GF(2). For example, to calculate the syndrome of $(x^iR(x) \bmod x^n-1)$, we need only calculate $(x^iS(x) \bmod x^n-1) \bmod g(x)$. This is done by adding $(x^iS(x) \bmod x^n-1)$ to $g(x)$ if $(x^iS(x) \bmod x^n-1)$ is of degree $\geq n-k$; otherwise continue cyclic shifting $S(x)$ until its weight is of t or less.

THEOREM 10. If code V has rate $\frac{k}{n} = \frac{1}{t}$, then the only error patterns which are not 1-step P.D. are of the following form:

$$x^j(b_o+b_1x^k+b_2x^{2k}+\ldots+b_{t-1}x^{(t-1)k});$$

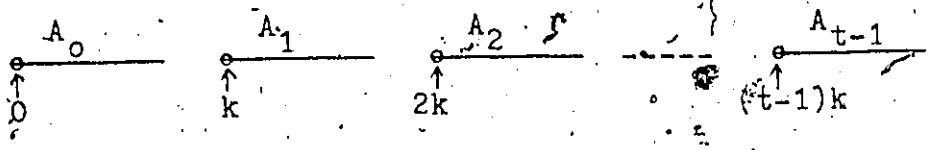
for $j = 0, 1, \ldots, k-1$ and $b_i \in GF(p)$.

Proof: Since $\frac{k}{n} = \frac{1}{t} < \frac{1}{t-1}$, hence by THEOREM 9 every error pattern of weight strictly less than t is 1-step P.D.. It is enough to consider those error patterns of weight t which are of the following type:

$$E(x) = b_o+b_1x^{a_1}+b_2x^{a_2}+\ldots+b_{t-1}x^{a_{t-1}}.$$

Suppose E(x) is not 1-step P.D., then from THEOREM 9, we have $a_{i+1}-a_i \leq k$ and $n-a_{t-1} \leq k$ for $i=0,1,\ldots,t-2$ and $a_o=0$.

Since n = kt, we can divide the n-bit-positions into t parts, each with k-bit-positions; say



It is obvious that each ~~a_i~~ lies in each A_i for i=0,1,...,t-1. If the gap between any two errors is strictly less than k, then there are only two possibilities: either two errors lie in the same A_i for some i or E(x) has a gap of length $\geq k$. Both of these two possibilities will make E(x) 1-step P.D. and this contradicts the assumption. Thus $a_i = ik$ for i=1,2,...,t-1. By the cyclic proprty, $x^j(b_0+b_1x^k+b_2x^{2k}+\ldots+b_{t-1}x^{(t-1)k})$ are not 1-step P.D. Since the period of this cycle is k, there are only k such error patterns which are not 1-step P.D.

Q.E.D.

2.3 2-step permutation decodable binary codes

2.3.1 Case of 2-error-correcting codes

Suppose code V with error-correcting-capability t=2 is not 1-step P.D. and $\frac{k}{n} > \frac{1}{2}$. We have $k < n < 2k$ and hence n

can be written as $n = k+i$ for some positive integer i with $0 < i \leq k-1$. Suppose $E(x) = 1+x^a$ is not 1-step P.D. By THEOREM 9, $k \geq a \geq n-k = i$ and hence $2k \geq 2a \geq 2i$. (note $2i < n$ for otherwise we have $2i \geq n = k+i \Longrightarrow i \geq k$). Therefore, either $n > 2a \geq 2i$ or $0 < 2a-n \leq k-i$. If $i > \frac{k}{2}$, then either $n > 2a > k$ ------ (1)

or $0 < 2a-n \leq k-i < n-k$ ------ (2).

Conditions (1) and (2) can be interpreted as follows:

If $E^2(x)$ mod x^n-1 is expressed as $E^2(x)$ mod $x^n-1 \equiv 1+x^b$, then either $b < n-k$ or $n > b > k$. In either case, $E^2(x)$ mod x^n-1 always has a gap of length $\geq k$. That is, $E(x)$ is 2-step P.D..

On the other hand, if $i \leq \frac{k}{2}$, then the error pattern $E(x) = 1+x^i$ is not 1-step P.D. since $n-k = i \leq \frac{k}{2}$ and $n-i = k+i-i = k$.

Now $E^2(x)$ mod $x^n-1 \equiv 1+x^{2i}$. But $2i \leq k$ and $n-2i = k+i-2i = k-i < k$. That is, $E^2(x)$ mod $x^n-1 \equiv 1+x^{2i}$ does not have a gap of length $\geq k$. Hence $E(x) = 1+x^i$ is not 2-step P.D. In other words, if $i \leq \frac{k}{2}$ or $n \leq k+\frac{k}{2} = \frac{3k}{2}$, code V is not 2-step P.D..

These results can be summarized as follows:

THEOREM 11. Suppose $t=2$ and code V has rate $\frac{k}{n} > \frac{1}{2}$.

Code V is 2-step P.D. iff $\frac{k}{n} < \frac{2}{3}$.

As an example, we consider the $(63, 42, 2)$ binary cyclic code. Since $\frac{k}{n} = \frac{2}{3}$, it is not 2-step P.D. by THEOREM 11. One can check that the error pattern $1+x^{21}$ is not 2-step P.D. However, we have the following result:

THEOREM 12. Suppose code V has rate $\frac{k}{n} = \frac{2}{3}$.

Then $x^j(1+x^{\frac{k}{2}}) \bmod x^n-1$ are the only error patterns which are not 2-step P.D.

Proof: Let $E(x) = 1+x^a$ be an error pattern which is not 1-step P.D. Then we have

(i) If $n-k < a < k$, then $2(n-k) < 2a < 2k$. But $n = k+\frac{k}{2}$ and $n-k = \frac{k}{2}$, so either $n > 2a > k$ or $2a-n < \frac{k}{2} = n-k$. In either case, $E(x) = 1+x^a$ is 2-step P.D.

(ii) If $a = n-k = \frac{k}{2}$, then $2a = k > n-k$.
$\therefore E(x) = 1+x^{\frac{k}{2}}$ is not 2-step P.D.

(iii) If $a = k$, then $2a = 2k$ and hence $2a-n = \frac{k}{2} = n-k$.
$\therefore E(x) = 1+x^k$ is not 2-step P.D.

Since $1+x^k$ is a cyclic shift of $1+x^{\frac{k}{2}}$, thus the only error patterns which are not 2-step P.D. are $x^j(1+x^{\frac{k}{2}}) \bmod x^n-1$.

Q.E.D.

2.3.2 Case of 4-error-correcting codes

THEOREM 13. Suppose code V is an (n, k, t=4) binary cyclic code with rate $\frac{1}{4} < \frac{k}{n} < \frac{1}{3}$. Then code V is 2-step P.D.

Proof: Let $E(x) = 1+x^{a_1}+x^{a_2}+x^{a_3}$ be an error pattern which is not 1-step P.D. By THEOREM 9, $a_{i+1}-a_i \leq k$ and $n-a_3 \leq k$, for $i=0,1$ and $a_0=0$. Since $\frac{1}{4} < \frac{k}{n} < \frac{1}{3}$, we have $4k > n > 3k$ and hence we can write $n = 3k+i$ and $n-k = 2k+i$ for some positive integer $i \leq k-1$.

$a_3-a_1 \leq 2k$ implies $a_1 \geq a_3-2k \geq i$. Similarly, $a_2 \geq k+i$; so $k \geq a_1 \geq i$, $2k \geq a_2 \geq k+i$ and $3k \geq a_3 \geq 2k+i$. Thus we have

$$\left.\begin{array}{r} 2i \leq 2a_1 \leq 2k \\ 2k+2i \leq 2a_2 \leq 4k \\ 4k+2i \leq 2a_3 \leq 6k \end{array}\right\} \text{---(*) which implies either}$$

$$\left.\begin{array}{r} 2i \leq 2a_1 \leq 2k \\ 2k+2i \leq 2a_2 < n \\ k+i \leq 2a_3-n \leq 3k-i \end{array}\right\} \text{---(i) or} \quad \left.\begin{array}{r} 2i \leq 2a_1 \leq 2k \\ 0 < 2a_2-n \leq k-i \\ k+i \leq 2a_3-n \leq 3k-i \end{array}\right\} \text{---(ii)}$$

In (i) we have $2a_2-(2a_3-n) \geq k+i > k$.

For if $2a_2-(2a_3-n) < k+i$, then $2a_2-2a_3+n < k+i$.

So $2a_3 > 2a_2+n-k-i = 2a_2+3k+i-k-i = 2a_2+2k$.

Therefore, $2a_3 > 2a_2+2k$; this is impossible since $a_3-a_2 \leq k$. Also (i) implies either $2a_3-n < 2a_1$ or $2a_3-n > 2a_1$. Thus, in case (i), if we express $E^2(x) \bmod x^n-1 \equiv 1+x^{b_1}+x^{b_2}+x^{b_3}$, then either the gap

between b_2 and b_3 is of length $\geq k$ or a_o and b_1 has a gap of length $\geq k$.

As for the case (ii), we shall show that $2a_1-(2a_2-n) \geq k+i$. Since $2a_2 \geq 2k+2i > n$, $a_2 = k+i+j$ where $j > \frac{k-i}{2}$. Therefore $a_1 \geq i+j$; so we have

$$2a_1 \geq 2i+2j > 2i+k-i = k+i \text{ ----------(1)}$$

Furthermore, $2a_2 = 2k+2i+2j > n$ and

$$2a_2-n = 2k+2i+2j-3k-i = i+2j-k \text{ ------(2)}$$

On the other hand, $2a_2 \leq 4k \Rightarrow 2a_2-n \leq k-i$ --(3)

Combining (1), (2) and (3), we have $2a_1 > 2a_2+n$ and $2a_1-(2a_2-n) \geq 2i+2j-(i+2j-k) = k+i$.

Finally, we note that if $2a_3-n < 2a_1$, then $2a_3-n < 2a_1 \leq 2k < n-k$. Thus, in case (ii), if $E^2(x) \bmod x^n-1 \equiv 1+x^{b_1}+x^{b_2}+x^{b_3}$, then either the gap between b_1 and b_2 is of length $\geq k$ or $b_3 < n-k$.

$\therefore E(x)$ is 2-step P.D. in either (i) or (ii).

Q.E.D.

2.3.3 Case of 6-error-correcting codes

THEOREM 14. Suppose code V is an (n, k, t=6) binary cyclic code with rate $\frac{1}{6} < \frac{k}{n} < \frac{1}{5}$. Then code V is 2-step P.D.

Proof: From $\frac{1}{6} < \frac{k}{n} < \frac{1}{5}$, we can write $n = 5k+i$ and $n-k = 4k+i$ for some positive integer $i \leq k-1$. By THEOREM 9, $a_{i+1}-a_i \leq k$ and $n-a_5 \leq k$, for $i=0,1,2,3,4$; $a_0=0$. $a_5-a_1 \leq 4k$ implies $a_1 \geq n-k-4k = i$; consequently, we have $jk \geq a_j \geq (j-1)k+i$ and $2jk \geq 2a_j \geq 2(j-1)k+2i$. For $j \geq 3$, $6k \geq 2a_j \geq 4k+2i$; this implies either

$$\left.\begin{array}{r} 2i \leq 2a_1 \leq 2k \\ 2k+2i \leq 2a_2 \leq 4k \\ 4k+2i \leq 2a_3 < n \\ k+i \leq 2a_4-n \leq 3k-i \\ 3k+i \leq 2a_5-n \leq 5k-i \end{array}\right\}\text{---(1) or}\quad \left.\begin{array}{r} 2i \leq 2a_1 \leq 2k \\ 2k+2i \leq 2a_2 \leq 4k \\ 0 < 2a_3-n \leq k-i \\ k+i \leq 2a_4-n \leq 3k-i \\ 3k+i \leq 2a_5-n \leq 5k-i \end{array}\right\}\text{---(2)}$$

In (1), we have $2a_3-(2a_5-n) \geq k+i$. For if $2a_3-(2a_5-n) < k+i$, then $2a_5 > 2a_3+n-k-i = 2a_3+4k$ and hence $a_5-a_3 > 2k$ which is impossible since E(x) is not 1-step P.D. If $2a_2$ lies between $2a_3$ and $(2a_5-n)$, then $2a_1$ and $2a_4-n$ lie in a length $\geq 3k$ positions. In other words, E(x) with (1) is 2-step P.D.

In (2) we shall show that $2a_1-(2a_3-n) \geq k+i$.

$a_3 = 2k+i+j$ for some positive integer j since $2a_3 > 4k+2i$. Therefore $a_1 \geq i+j$; so we have

$$2a_1 \geq 2i+2j > 2i+k-i \quad \text{----------(3)}$$

Furthermore, $2a_3 = 4k+2i+2j$ and $2a_3-n = i+2j-k$ --(4)

(3) and (4) show that $2a_1-(2a_3-n) \geq i+k$.

Finally, if $2a_4-n$ lies between $2a_1$ and $2a_3-n$, then $2a_2$ and $2a_5-n$ lie in a length $\geq 3k$ positions since $2a_1 \leq 2k$ and $n-2a_1 \geq 3k+i$. Thus E(x) with (2) is 2-step P.D. That is, code V is 2-step P.D.

Q.E.D.

2.4 3-step permutation decodable binary codes

2.4.1 Case of 2-error-correcting codes

THEOREM 15. Suppose code V is a double-error-correcting code with k odd and $n = k+\frac{k}{2}-\frac{1}{2}$. Then code V is 3-step P.D.

Proof: We first note that $k \geq 3$ for otherwise n will be even or $n = k$. Let $E(x) = 1+x^a$ be an error pattern which is not 1-step P.D. Then we have to consider the following 3 cases:

(i) $k-1 \geq a \geq n-k+j$; where $j \geq 1$.

This gives $2k-2 \geq 2a \geq 2(n-k)+2j = 2(\frac{k}{2}-\frac{1}{2})+2j \geq k$.

$\therefore$ either $n \geq 2a \geq k-1+2j \geq k$ or

$0 < 2a-n \leq 2k-2-k-\frac{k}{2}+\frac{1}{2} = \frac{k}{2}-\frac{3}{2} < n-k$.

Thus E(x) is 2-step P.D.

(ii) If $a = \frac{k}{2}-\frac{1}{2}$, then $n-k < 2a = k-1 < k$.

Thus E(x) is not 2-step P.D. But $4a = 2k-2 \geq n$

(if $2k-2 \leq n$, then $2k-2 \leq k+\frac{k}{2}-\frac{1}{2}$; this implies that $k \leq 3$), so $4a-n = \frac{k}{2}-\frac{3}{2} < n-k$.

$\therefore E(x) = 1+x^{\frac{k}{2}-\frac{1}{2}}$ is 3-step P.D.

(iii) If $a = k$, then $E(x)$ is not 2-step P.D.

But $4a = 4k > 2n$ and $4a-2n = k+i > k$.

$\therefore E(x)$ is 3-step P.D.

Q.E.D.

THEOREM 16. Suppose code V is a double-error-correcting code with $n = 3b$, $k = 2b+1$; where b is some positive integer. Then code V is 3-step P.D. if we do not consider the error patterns: $x^j(1+x^b) \bmod x^n-1$.

Proof: Since $(1+x^b)^2 = 1+x^{2b}$ and $(1+x^{2b})^2 \bmod x^n-1 \equiv 1+x^b$, $x^j(1+x^b) \bmod x^n-1$ and $x^j(1+x^{2b}) \bmod x^n-1$ are not 3-step P.D. In fact, $1+x^{2b}$ is a cyclic shift of $1+x^b$. Now let $E(x) = 1+x^a$ be an error pattern which is not 1-step P.D. Then $k \geq a \geq n-k = b-1$.

If $b+1 \leq a \leq 2b-1$, then $2b+2 \leq 2a \leq 4b-2$.

$\therefore$ either $n < 2a \geq 2b+2 > k$ or $0 < 2a-n \leq b-2 < n-k$.

In either case, $E(x)$ is easily seen to be 2-step P.D.

If $a = n-k = b-1$, then $2a = 2b-2$ and $4a = 4b-4$.

$\therefore 4a-n = 4b-3b-4 = b-4 < n-k$ and hence $E(x) = 1+x^{b-1}$ is 3-step P.D. Now if $a = k = 2b+1$, then we can show that $4a-2n = 2b+2 > k$. $\therefore E(x) = 1+x^{2b+1}$ is 3-step P.D.

Q.E.D.

Example 3. Consider the BCH code with parameters n=31, k=21, t=2. Since $n = 21 + \frac{21}{2} - \frac{1}{2} = 31$ and t=2, it is 3-step P.D. by THEOREM 15. The only error patterns which require 3-step P.D. are $x^j(1+x^{10}) \bmod x^{31}-1$ and $x^j(1+x^{21}) \bmod x^{31}-1$.

Example 4. Consider the (63, 43, 2) binary cyclic code. Since $n = 3(21)$ and $k = 2(21)+1$, hence by THEOREM 16, $x^j(1+x^{21}) \bmod x^{63}-1$ are the only error patterns which are not 3-step P.D.

2.4.2 Case of 3-error-correcting codes

Let code V be an (n, k, t=3) binary cyclic code with rate $\frac{1}{2} < \frac{k}{n} < \frac{4}{7}$ so that we can write $n = k + \frac{3}{4}k+i$ and $n-k = \frac{3}{4}k+i$, where $0 < i < \frac{k}{4}$ and $k \geq 4$. Then we have the following 3 lemmas.

Lemma 10. The error pattern $E(x) = 1+x^{a_1}+x^{a_2}$ such that

$$\left.\begin{aligned} a_1 &\leq k \\ a_2-a_1 &\leq k \\ n-a_2 &\leq k \\ 2a_1 &\leq k \\ 2(a_2-a_1) &\leq k \\ n-2a_2 &\leq k \end{aligned}\right\} \text{----(*)} \quad \text{is 3-step P.D.}$$

Proof: From (*), we have $a_1 \leq \frac{k}{2}$ and $2(a_2-a_1) \leq k$.

But $n \geq 2a_2 \geq 2(n-k) = \frac{3}{2}k+2i$; therefore

$\frac{3}{2}k+2i-2a_1 \leq 2(a_2-a_1) \leq k$; hence $\frac{k}{2} \geq a_1 \geq \frac{k}{4}+i$;

or equivalently, $2k \geq 4a_1 \geq k+4i$ ---------(1)

(note $k+4i < n$. For if $k+4i \geq n$, then $4i \geq \frac{3}{4}k+i \Rightarrow i \geq \frac{k}{4}$).

(1) yields either $n > 4a_1 \geq k+4i > k$ ------(2)

or $\frac{k}{4} - i \geq 4a_1 - n > 0$ ----------(3)

Furthermore, $4k > 4a_2 \geq 2k+k+4i = 3k+4i > n$.

$\therefore 2k - \frac{k}{4} - i > 4a_2 - n \geq k + \frac{k}{4} + 3i > k$ ---------(4).

(3) and (4) show that $4a_2 - n - (4a_1 - n) \geq k+4i > k$ ----(5)

Thus, the conditions (2), (4) and the conditions (3), (5) show that $E^4(x) \equiv 1+x^{4a_1}+x^{4a_2} \bmod x^n-1$ always has a gap of length $\geq k$.

Hence $E(x) = 1+x^{a_1}+x^{a_2}$ with (*) is 3-step P.D.

Q.E.D.

Lemma 11. The error pattern $E(x) = 1+x^{a_1}+x^{a_2}$ with

$$\left.\begin{aligned} a_1 &\leq k \\ a_2 - a_1 &\leq k \\ n - a_2 &\leq k \\ 2a_1 - n &\leq k \\ 2a_2 - n - (2a_1 - n) &< k \\ 2(n - a_2) &\leq k \end{aligned}\right\} \text{----(**) is 3-step P.D.}$$

Proof: From (**), we have $a_2 > a_1 > n-k$ and $2a_1 - n < 2k - k - \frac{3}{4}k - i$

$= \frac{k}{4} - i$. $\therefore 4a_1 - 2n \leq \frac{k}{2} - 2i < n-k$ -------(1)

But $2a_1 - n - (2a_1 - n) \leq k \Rightarrow a_2 - a_1 \leq \frac{k}{2}$ or $a_2 \leq k + \frac{k}{2} = \frac{3}{2}k$,

hence $2a_2 \leq 3k$; so $2a_2-n \leq k+\frac{k}{4}-i$.

$$4a_2-2n \leq 2k+\frac{k}{2}-2i \text{ ----------(2).}$$

By (**), $4a_2-2n \geq 2(n-k) \geq k+\frac{k}{2}+2i$ ----------(3).

(2) and (3) imply either $n-k \geq \frac{3}{4}k-3i \geq 4a_2-3n \geq 0$ (4).

or $n \geq 4a_2-2n \geq k+\frac{k}{2}+2i$ (5).

If $E^4(x) \equiv 1+x^{4a_1}+x^{4a_2} \bmod x^n-1 \equiv 1+x^{b_1}+x^{b_2}$,

then conditions (1) and (4) show that $b_2 < n-k$ and conditions (1) and (5) show that a gap between b_1 and b_2 is of length $\geq k$. $\therefore E(x)$ with (**) is 3-step P.D.

Q.E.D.

Lemma 12. The error pattern $E(x) = 1+x^{a_1}+x^{a_2}$ with

$$\left.\begin{aligned} a_1 &\leq k \\ a_2-a_1 &\leq k \\ n-a_2 &\leq k \\ 2a_1 &\leq k \\ 2a_2-n-2a_1 &\leq k \\ 2(n-a_1) &\leq k \end{aligned}\right\} \text{----(***) is 3-step P.D.}$$

Proof: By (***), $a_1 \leq \frac{k}{2}$ and $a_1 \geq a_2-k \geq n-k-\frac{k}{2} = k+\frac{3}{4}k-\frac{k}{2}-k+i$

$= \frac{k}{4}+i$. $\therefore \frac{k}{2} \geq a_1 \geq \frac{k}{4}+i$ and $k \geq 2a_1 \geq \frac{k}{2}+2i$.

Hence $2k \geq 4a_1 \geq k+4i$; so either

$$n-k \geq \frac{k}{4}-i \geq 4a_1-n \geq 0 \text{ --------(1)}$$

or $n \geq 4a_1 \geq k+4i$ ----------(2).

Also, we have either $n-k \succ \frac{3}{4}k-3i \geq 4a_2-3n \succ 0$ ----(3)

or $n \succ 4a_2-2n \geq k+\frac{k}{2}+2i$ ----(4).

The above discussions show that if we express $E^4(x) \bmod x^n-1 \equiv 1+x^{b_1}+x^{b_2}$, there are 4 possibilities to be considered, namely: (1) and (3), (1) and (4), (2) and (4), (2) and (3). From the first 3 possibilities, it can be easily checked that $E^4(x) \bmod x^n-1$ always has a gap of length $\succ k$. As for conditions (2) and (3), we have $n \succ 4a_1 \geq k+4i$ and $\frac{3}{4}k-3i \geq 4a_2-3n \succ 0$. We shall show that $4a_1-(4a_2-3n) \succ k$. Suppose $4a_1-(4a_2-3n) \preceq k$. Then $4a_1 \leq 4a_2+k-3n \leq 4(a_1+k)+k-3n = 4a_1+5k-3n$ since $a_2-a_1 \leq k \Rightarrow 4a_2 \leq 4(a_1+k)$. Hence $5k-3n \geq 0$ or $5k \geq 3n$. That is, $\frac{k}{n} \geq \frac{3}{5} \succ \frac{4}{7}$. Contradict to the fact that $\frac{k}{n} \prec \frac{4}{7}$. Therefore, $4a_1-(4a_2-3n) \succ k$. This shows that $E^4(x) \bmod x^n-1$ with conditions (2) and (3) is 3-step P.D.

Q.E.D.

THEOREM 17. Suppose code V is an (n, k, t=3) binary cyclic code with rate $\frac{1}{2} \prec \frac{k}{n} \prec \frac{4}{7}$. Then the error pattern

$E(x) = 1+x^{a_1}+x^{a_2}$ with

$a_1 \prec k$
$a_2-a_1 \leq k$
$n-a_2 \leq k$
$2a_2-n \prec k$
$2a_1-2(a_2-n) \leq k$
$n-2a_1 \leq k$

} ----(****) may not be 3-step P.D.

Proof: Let $E(x) = 1+x^{a_1}+x^{a_2}$ be an error pattern which is not 2-step P.D. There are only 4 cases such that $E^4(x) \bmod x^n-1$ has no gap of length $\geq k$. Namely: (*) in Lemma 10, (**) in Lemma 11, (***) in lemma 12 and (****). The first three cases have been shown that $E^4(x) \bmod x^n-1$ is 3-step P.D. So we need only consider the case (****). From (****), we have $k > a_1 \geq \frac{n-k}{2}$ and $n-k < a_2 \leq \frac{n+k}{2}$. Hence $2k > n > 2a_1 > n-k$; consequently, either $n < 4a_1 \geq \frac{3}{2}k+2i > k$ ----(1)

or $n > 4a_1-n > 0$ ---------(2).

Furthermore, $n < 2a_2 \leq n+k$ and $0 < 2a_2-n \leq k$; so either

$0 < 4a_2-2n < n$ ----(3) or $0 < 4a_2-3n \leq \frac{k}{4} - i$ ----(4).

Conditions (1) to (4) show that it is possible that $E^4(x) \bmod x^n-1$ may have no gap of length $\geq k$.

Q.E.D.

Example 5. Consider the Golay (23, 12, 3) code generated by $g(x) = 1+x^2+x^4+x^5+x^6+x^{10}+x^{11}$. Since $\frac{1}{2} < \frac{k}{n} = \frac{12}{23} < \frac{4}{7}$, then by THEOREM 17, the error pattern $E(x) = 1+x^{a_1}+x^{a_2}$ which may not be 3-step P.D. has $12 \geq a_1 \geq \frac{1}{2}(23-12) = 5\frac{1}{2}$ and $11 < a_2 \leq \frac{1}{2}(23+12) = 17\frac{1}{2}$. In fact, such error patterns are found as follows:

$E_1(x) \equiv x^j(1+x^7+x^{15}) \bmod x^{23}-1$, $E_2(x) \equiv x^j(1+x^8+x^{15}) \bmod x^{23}-1$

and $E_3(x) \equiv x^j(1+x^8+x^{16}) \bmod x^{23}-1$.

Since $E_1^2(x) \equiv x^{2j}(1+x^7+x^{14}) \bmod x^{23}-1$,

$E_2^2(x) \equiv x^{2j}(1+x^7+x^{16}) \bmod x^{23}-1$ and $E_3^2(x) \equiv x^{2j}(1+x^9+x^{14}) \bmod x^{23}-1$;

we have $E_1^4(x) \equiv x^{4j}(1+x^5+x^{14}) \bmod x^{23}-1$,

$E_2^4(x) \equiv x^{4j}(1+x^9+x^{14}) \bmod x^{23}+1$ and $E_3^4(x) \equiv x^{4j}(1+x^9+x^{18}) \bmod x^{23}-1$.

Thus $E_1(x)$, $E_2(x)$ and $E_3(x)$ are not 3-step P.D. Note that $E_i^8(x) \bmod x^{23}-1$ for $i=1,2,3$ always has a gap of length $\leq k$. This means that the Golay code is 4-step P.D.

Example 6. Consider the (63, 36, t=3) BCH code. THEOREM 17 is not applicable here since $\frac{k}{n} = \frac{4}{7}$. The error pattern $1+x^{17}+x^{20}$ which satisfies (*) in Lemma 10 can be easily shown that it is not 3-step P.D. This example shows that the bound for the rate $\frac{k}{n}$ of an existent code V with t=3 cannot be improved.

2.5 2-step permutation decoding for binary codes with t even

To obtain the bound for the rate of an existent code which is higher step permutation decodable needs complicated computation, especially for those with t very large. However, for codes which are 2-step P.D. and have even error-correcting capability, we have the following result.

THEOREM 18. Let V be a binary (n, k, t) cyclic code with t even, k odd and $tk > n \geq tk - \frac{k}{2} + \frac{1}{2}$. Then code V is 2-step P.D.

Before we give the proof of this theorem, we first prove the following 5 lemmas which are based on the fact that code V is a binary (n, k, t) cyclic code with t even, k odd and $tk > n \geq tk - \frac{k}{2} + \frac{1}{2}$.

Lemma 13. (i) Every error pattern of weight strictly less than t is 1-step P.D.

(ii) The only error patterns which are not 1-step P.D. are of weight t and of the following type:

$E(x) = 1 + x^{a_1} + x^{a_2} + \ldots + x^{a_{t-1}}$ with $a_{i+1} - a_i \leq k$ and $n - a_{t-1} \leq k$ for $i = 0, 1, \ldots, t-2$ and $a_0 = 0$.

(iii) $jk \geq a_j \geq (j - \frac{1}{2})k + \frac{1}{2}$ for $j = 1, 2, \ldots, t-1$; a_j as in (ii)

Proof: (i) Since $n \geq tk - \frac{k}{2} + \frac{1}{2} = tk - k + \frac{k}{2} + \frac{1}{2} = (t-1)k + \frac{k}{2} + \frac{1}{2}$, $n > (t-1)k$ or $\frac{k}{n} < \frac{1}{t-1}$. Every error pattern of weight strictly less than t is 1-step P.D.

(ii) It follows from the cyclic property of the code V and THEOREM 9.

(iii) From (ii), we have $a_{i+1} - a_i \leq k$ and $n - a_{t-1} \leq k$. It follows that $jk \geq a_j$, for $j = 1, 2, \ldots, t-1$.

Since $n \geq tk - \frac{k}{2} + \frac{1}{2} = (t-1)k + \frac{k}{2} + \frac{1}{2}$,

$n-k \geq tk - \frac{3}{2}k + \frac{1}{2} = (t-2)k + \frac{k}{2} + \frac{1}{2}$. Also, $n-a_{t-1} \leq k$ implies that $a_{t-1} \geq n-k \geq (t-1)k - \frac{k}{2} + \frac{1}{2}$ and $a_{t-1}-a_1 \leq (t-2)k$.

So we have $a_1 \geq a_{t-1}-(t-2)k \geq n-k-(t-2)k$

$\geq tk - \frac{3}{2}k + \frac{1}{2} - tk + 2k = (1 - \frac{1}{2})k + \frac{1}{2}$.

$a_{t-1}-a_2 \leq (t-3)k \Rightarrow a_2 \geq a_{t-1}-(t-3)k \geq (2 - \frac{1}{2})k + \frac{1}{2}$;

similarly, $a_j \geq (j - \frac{1}{2})k + \frac{1}{2}$ for $j=1,2,\ldots,t-1$.

$\therefore$ we have $jk \geq a_j \geq (j - \frac{1}{2})k + \frac{1}{2}$, for $j=1,2,\ldots,t-1$.

Q.E.D.

Lemma 14. $k+1 \leq 2a_j < n-k$ for $1 \leq j \leq \frac{t}{2} - 1$.

Proof: By Lemma 13 (iii), we have $jk \geq a_j \geq (j - \frac{1}{2})k + \frac{1}{2}$

and hence $2jk \geq 2a_j \geq 2(j - \frac{1}{2})k + 1$, for $j=1,2,\ldots,t-1$.

For $j = \frac{t}{2} - 1$, we have $2a_j \leq 2(\frac{t}{2} - 1)k = (t-2)k < n-k$ ---(1).

Furthermore, $2a_1 \geq 2(1 - \frac{1}{2})k + 1 = k+1$ ----------(2).

Combining (1) and (2), we have

$k+1 \leq 2a_j < n-k$ for $1 \leq j \leq \frac{t}{2} - 1$.

Q.E.D.

Lemma 15. $k+1 \leq 2a_j - n < n-k$ for $\frac{t}{2} + 1 \leq j \leq t-1$.

Proof: By Lemma 13 again, we have

$2jk \geq 2a_j \geq 2(j-\frac{1}{2})k+1$ for $j=1,2,\ldots,t-1$.

For $j \geq \frac{t}{2}+1$, $2a_j \geq 2(\frac{t}{2}+1-\frac{1}{2})k+1 = tk+k+1 > n$.

$\therefore 2a_j-n \geq tk+k+1-n \geq tk+k+1-tk = k+1$.

When $j=t-1$, $2a_j \leq 2(t-1)k = 2tk-2k$ and therefore

$2a_j-n \leq 2tk-2k-tk+\frac{k}{2}-\frac{1}{2} = (t-2)k+\frac{k}{2}-\frac{1}{2} < n-k$.

This means that $k+1 \leq 2a_j-n < n-k$ for $\frac{t}{2}+1 \leq j \leq t-1$.

Q.E.D.

Lemma 16. $k+1 \leq 2a_j \bmod n < n-k$ for $j=1,2,\ldots,\frac{t}{2}-1,\frac{t}{2}+1,\ldots,t-1$.

Proof: Combining Lemma 14 and Lemma 15, we get this lemma immediately.

Q.E.D.

Lemma 17. For $j=\frac{t}{2}$, either $0 < 2a_{\frac{t}{2}}-n \leq k$ or $n-k \leq 2a_{\frac{t}{2}} < n$.

Proof: For $j=\frac{t}{2}$, from Lemma 13 (iii), we have

$2(\frac{t}{2})k \geq 2a_j \geq 2(\frac{t}{2}-\frac{1}{2})k+1$, i.e. $tk \geq 2a_j \geq (t-1)k+1$.

This shows that either $0 < 2a_{\frac{t}{2}}-n \leq k$ or $n-k \leq 2a_{\frac{t}{2}} < n$.

Q.E.D.

Proof of THEOREM 18: By Lemma 13, the error patterns which are not 1-step P.D. are of the form

$$E(x) = 1+x^{a_1}+x^{a_2}+\ldots+x^{a_{t-1}}.$$

Express $E^2(x) \bmod x^n-1 \equiv 1+x^{b_1}+x^{b_2}+\ldots+x^{b_{t-1}}$,

from Lemma 16 and Lemma 17 we have either $b_{t-1} < n-k$ or if $b_{t-1} \geq n-k$, then $b_1 \geq k+1$.

In either case, $E^2(x) \bmod x^n-1$ is 2-step P.D. Thus, we have proved generally that the theorem is true.

Q.E.D.

THEOREM 19. Let V be a binary (n, k, t) cyclic code with t even, k even and $tk > n > tk-\frac{k}{2}$. Then code V is 2-step P.D.

Proof: Since $n > tk-\frac{k}{2}$, $n = tk-\frac{k}{2}+i > tk-\frac{k}{2}+\frac{1}{2}$; where i is some positive integer with $i < \frac{k}{2}$. Hence Lemma 13 to Lemma 17 hold here so we have this theorem.

Q.E.D.

THEOREM 18 and THEOREM 19 can be restated as follows: Suppose V is a binary (n, k, t) cyclic code with t even. If $\frac{k}{n} < \frac{2}{2t-1}$, then V is 2-step P.D.

2.6 Decoding procedure for permutation decodable codes

On receiving the word R(x), we divide R(x) by g(x) and $x^{n-1}R(\frac{1}{x})$ by g*(x) simultaneously; where g*(x) is the reciprocal polynomial of g(x). That is, $g^*(x) = x^{n-k}g(\frac{1}{x})$.

Correction can be made without cyclic shifting R(x) if errors of E(x) are confined to the first or last n-k check positions. The worst is that some errors in E(x) lie in the first and last n-k check positions respectively.

If the code V is 1-step P.D., then the errors of E(x), will be brought to the first or last n-k check positions with at most n-(k+1) cyclic shifts of R(x). The error pattern which requires n-(k+1) cyclic shifts of R(x) has only one gap of length k.

If the code V is 2-step P.D. and $(x^i R(x) \bmod x^n-1) \bmod g(x)$ has weight $\leq t$ for $i=0,1,\ldots,n-(k+1)$, then we consider $(x^i R^p(x) \bmod x^n-1) \bmod g(x)$. The errors can be found out with at most $2(n-k-1)$ cyclic shifts of R(x) and $R^p(x)$ totally.

In general, if the code V is s-step P.D., then at most $s(n-k-1)$ cyclic shifts of R(x), $R^p(x)$, ..., $R^{p^{s-1}}(x)$ totally will complete the decoding procedure.

Suppose we want to decode the (63, 43, 2) binary cyclic code. We have shown that $x^j(1+x^{21}) \bmod x^{63}-1$ are the only error patterns which are not 3-step P.D. Thus, if the syndrome of R(x) matches one of the syndromes of $x^j(1+x^{21}) \bmod x^{63}-1$, then the error pattern can be found. Otherwise

at most 3(63-43-1) = 57 cyclic shifts of $R(x)$, $R^2(x)$, $R^4(x)$ totally will complete the decoding procedure.

Similarly, to decode the Golay (23, 12, 7) code, we can either proceed with the 4-step permutation decoding or with the 3-step permutation decoding together with matching the syndrome of $R(x)$ and the precalculated syndromes of $x^j(1+x^7+x^{15}) \bmod x^{23}-1$, $x^j(1+x^8+x^{15}) \bmod x^{23}-1$ and $x^j(1+x^8+x^{16}) \bmod x^{23}-1$ respectively.

APPENDIX

THEOREM A is a generalization of THEOREM 13 and THEOREM 14 in Chapter 2. The following Lemma and its corollaries simplify the proof of this theorem.

Lemma 18. Suppose code V is a binary (n, k, t) cyclic code with with rate $\frac{1}{t} < \frac{k}{n} < \frac{1}{t-1}$, t even and $t \leq 4$. Then

(i) Every error pattern of weight $< t$ is 1-step P.D.

(ii) If $E(x) = 1+x^{a_1}+x^{a_2}+\ldots+x^{a_{t-1}}$ is an error pattern which is not 1-step P.D., then $jk \geq a_j \geq (j-1)k+i$ for some i, $0 < i \leq k-1$ and for $j = 1,2,\ldots,t-1$.

Proof: (i) Since $\frac{k}{n} < \frac{1}{t-1}$, every error pattern of weight $< t$ is 1-step P.D. by THEOREM 9 in Chapter 2.

(ii) If $E(x) = 1+x^{a_1}+x^{a_2}+\ldots+x^{a_{t-1}}$ is an error pattern which is not 1-step P.D., then we have $a_{j+1}-a_j \leq k$ and $n-a_{t-1} \leq k$ for $j = 0,1,\ldots,t-2$; $a_0=0$. Thus we have $a_j \leq jk$. On the other hand, $a_{t-1}-a_j \leq (t-1-j)k$, $\therefore a_j \geq a_{t-1}-(t-1-j)k \geq (n-k)-(t-1-j)k$. Since $\frac{1}{t} < \frac{k}{n} < \frac{1}{t-1}$, we can write $n = (t-1)k+j$ and hence $n-k = (t-2)k+i$ for some positive integer

$i \leq k-1$. Therefore, $a_j \geq (n-k)-(t-1-j)k$ implies that

$a_j \geq (t-2)k+i-(t-1-j)k = (j-1)k+i$.

$\therefore jk \geq a_j \geq (j-1)k+i$ for $j = 1,2,\ldots,t-1$.

Q.E.D.

Corollary L.18.1. $2i \leq 2a_j \leq (t-2)k \leq n-k$ for $1 \leq j \leq \frac{t}{2}-1$.

Proof: By Lemma 18, $jk \geq a_j \geq (j-1)k+i$ and hence

$2jk \geq 2a_j \geq 2(j-1)k+2i$.

For $j = 1$, $2k \geq 2a_1 \geq 2i$ .....(1).

For $j = \frac{t}{2}-1$, $2(\frac{t}{2}-1)k \geq 2a_j \geq 2(\frac{t}{2}-1-1)k+2i$;

i.e. $(t-2)k \geq 2a_j \geq (t-4)k+2i$ ....(2).

Combining (1) and (2), we have

$n-k \geq (t-2)k \geq 2a_j \geq 2i$ for $j = 1,2,\ldots,\frac{t}{2}-1$.

Q.E.D.

Corollary L.18.2. $ki \leq 2a_j-n \leq (t-1)k-i$ for $\frac{t}{2}+1 \leq j \leq t-1$.

Proof: By Lemma 18 again, $2jk \geq 2a_j \geq 2(j-1)k+2i$.

For $j = \frac{t}{2}+1$, $2a_j \geq 2(\frac{t}{2}+1-1)k+2i = tk+2i \geq n$;

$\therefore 2a_j-n \geq tk+2i-(t-1)k-i = k+i$.

Thus $2a_j-n \geq k+i$ for $j \geq \frac{t}{2}+1$ .....(1).

Furthermore, for $j = t-1$, $2a_j \leq 2(t-1)k = 2tk-2k$;

$\therefore 2a_j-n \leq 2tk-2k-(t-1)k-i = (t-1)k-i$ ....(2).

From (1) and (2), we have

$k+i \leq 2a_j - n \leq (t-1)k-i$ for $\frac{t}{2}+1 \leq j \leq t-1$.

Q.E.D.

Corollary L.18.3. For $j = \frac{t}{2}$, either $(t-2)k+2i \leq 2a_{\frac{t}{2}} < n$

or $0 < 2a_{\frac{t}{2}} - n \leq k-i$.

Proof: For $j = \frac{t}{2}$, we have

$2(\frac{t}{2}-1)k+2i \leq 2a_j \leq 2(\frac{t}{2})k = tk$ by Lemma 18 again.

Thus either $(t-2)k+2i \leq 2a_j < n$

or $0 < 2a_{\frac{t}{2}} - n \leq k-i$.

Q.E.D.

THEOREM A. Suppose code V is a binary (n, k, t) cyclic code with rate $\frac{1}{t} < \frac{k}{n} < \frac{1}{t-1}$, t even and $t \geq 4$. Then code V is 2-step P.D.

Proof: As in Lemma 18, we write $n = (t-1)k+i$ and hence $n-k = (t-2)k+i$ for some positive integer $i \leq k-1$.

By the cyclic property of the code V and Lemma 18 (i), any error pattern which is not 1-step P.D. is of the following type: $E(x) = 1+x^{a_1}+x^{a_2}+\ldots+x^{a_{t-1}}$.

Now suppose $E(x) = 1+x^{a_1}+x^{a_2}+\ldots+x^{a_{t-1}}$ is not 1-step P.D.

Consider $E^2(x) \equiv 1+x^{2a_1}+x^{2a_2}+\ldots+x^{2a_{t-1}} \bmod x^n-1$.

From the corollaries of Lemma 18, $E^2(x) \bmod x^n-1$ will give either

$$\left.\begin{array}{rl} 2i \leq & 2a_1 \leq 2k \\ 2k+2i \leq & 2a_2 \leq 4k \\ & \vdots \\ (t-4)k+2i \leq & 2a_{\frac{t}{2}-1} \leq (t-2)k \\ (t-2)k+2i \leq & 2a_{\frac{t}{2}} < n \\ & \vdots \\ (t-3)k+i \leq & 2a_{t-1}-n \leq (t-1)k-i \end{array}\right\} \quad \ldots\ldots (1)$$

or

$$\left.\begin{array}{rl} 2i \leq & 2a_1 \leq 2k \\ 2k+2i \leq & 2a_2 \leq 4k \\ & \vdots \\ (t-4)k+2i \leq & 2a_{\frac{t}{2}-1} \leq (t-2)k \\ 0 < & 2a_{\frac{t}{2}}-n \leq k-i \\ & \vdots \\ (t-3)k+i \leq & 2a_{t-1}-n \leq (t-1)k-i \end{array}\right\} \quad \ldots\ldots (2)$$

In (1), we have

(i) $2a_{\frac{t}{2}}-(2a_{t-1}-n) \geq k+i$. For if $2a_{\frac{t}{2}}-(2a_{t-1}-n) < k+i$, then $2a_{t-1} > 2a_{\frac{t}{2}}+n-k-i = 2a_{\frac{t}{2}}+(t-2)k$.

Therefore, $2a_{t-1}-2a_{\frac{t}{2}} > (t-2)k \Rightarrow a_{t-1}-a_{\frac{t}{2}} > (\frac{t}{2}-1)k$.

This contradicts the fact that E(x) is not 1-step P.D.

(ii) If $2a_{\frac{t}{2}-1}$ lies between $2a_{\frac{t}{2}}$ and $2a_{t-1}-n$, then

at most (t-4) errors will lie in a gap of length $\geq (t-3)k$ positions. This is because $2a_{t-1}-n \geq (t-3)k+i$ and hence the gap between $2a_o=0$ and $2a_{t-1}-n$ is of length $\geq (t-3)k+i-1 \geq (t-3)k$.

Thus in either (i) or (ii), $E^2(x) \bmod x^n-1$ always has a gap of length $\geq k$.

In (2), we have

(iii) $2a_1-(2a_{\frac{t}{2}}-n) \geq k+i$. For if $2a_1-(2a_{\frac{t}{2}}-n) < k+i$, then $2a_{\frac{t}{2}} > 2a_1-n-k-i$. This implies that $2a_{\frac{t}{2}}-2a_1 > (t-2)k$ or $a_{\frac{t}{2}}-a_1 > (\frac{t}{2}-1)k$. This gives a contradiction.

(iv) If $2a_{\frac{t}{2}+1}-n$ lies between $2a_{\frac{t}{2}}-n$ and $2a_1$, then we have at most (t-4) errors lying in a gap of length $\geq (t-3)k+i-1 \geq (t-3)k$ positions since $2a_1 \leq 2k$ and hence $n-2a_1 \geq (t-3)k+i$.

Thus either (iii) or (iv) implies that $E^2(x) \bmod x^n-1$ always has a gap of length $\geq k$.

From the above discussions in (1) and (2), we conclude that the code V is 2-step P.D.

Q.E.D.

Remark. THEOREM A does not hold for $t = 2$. We explain it as follows:

Suppose it is true for $t = 2$.

(i) Every double-error-correcting code with rate $\frac{k}{n} < 1$ is 2-step P.D. This will contradict THEOREM 11 and THEOREM 12 in Chapter 2.

(ii) In the proof of this theorem, the fact that either $(t-2)k+2i \leq 2a_{\frac{t}{2}} < n$ or $0 < 2a_{\frac{t}{2}} - n \leq k-i$ plays an important role. For $t = 2$, we have $n = k+i$ and hence $n-k = i$; we also have either $2i \leq 2a_1 < n$ or $0 < 2a_1 - n \leq k-i$. In particular, for $i = 1$, $n = k+1$ and $n-k = 1$. We may assume that $k \geq 4$. (For $k = 1$ or 3, n will be even; for $k = 2$, $\frac{k}{n} = \frac{2}{3}$ which has been discussed.) Thus we have $n-k < 2 \leq 2a_1 < n$ which does not imply that $2a_1$ must be greater than k. In other words, the range of i for $t = 2$ in THEOREM A is not the same as that for $t \geq 4$. That is, for $t = 2$, code V need not be 2-step P.D. for some particular i.

BIBLIOGRAPHY

[1] P.E. Allard, S.G.S. Shiva & S.E. Tavares, A Note on the Decomposition of Cyclic Codes into Cyclic Classes, Information and Control, 22, 1973, 100-106.

[2] E.R. Berlekamp, (1968), "Algebraic Coding Theory," McGraw-Hill, New York.

[3] Kaplansky, (1972), "Fields and Rings," The University of Chicago Press, Chicago.

[4] F.J. MacWilliams, (1964), Permutation Decoding of Systematic Codes. Bell Sys. Tech. J. 43, 485-505.

[5] _____, (1965), The structure and properties of binary cyclic alphabets, Bell Sys. Tech. J. 44, 303-333.

[6] H. Paley & P.M. Weichsel, (1964), "A First Course in ABSTRACT ALGEBRA," Holt Rinehart and Winston, Inc.

[7] W.W. Peterson & E.J. Weldon, Jr. (1972), "Error-correcting-Codes" M.I.T. Press, Cambridge and Wiley, New York.

[8] Lin Shu, (1972), "An Introduction to ERROR-CORRECTING-CODES," Prentice-Hall. Inc., Englewood Cliffs, New Jersey.

[9] S.E. Tavares, P.E. Allard & S.G.S. Shiva, On the Decomposition of Cyclic Codes into Cyclic Classes, Information and Control, 18, 1971, 342-354.