

UNIVERSITY OF NORTH CAROLINA
Department of Statistics
Chapel Hill, N. C.

Mathematical Sciences Directorate
Air Force Office of Scientific Research
Washington 25, D. C.

AFOSR Report No.

ON THE CONSTRUCTION OF BURST-ERROR-CORRECTING CODES

by

Alan John Gross

July, 1961

Contract No. AF 49(638)-213

Error correcting codes are constructed which correct errors occurring in bursts of a predetermined length. Binary, ternary and quintary codes are considered for single error bursts whereas only the binary codes are considered for the multiple burst case. These codes are constructed by use of Galois fields.

Qualified requestors may obtain copies of this report from the ASTIA Document Service Center, Arlington Hall Station, Arlington 12, Virginia. Department of Defense contractors must be established for ASTIA services, or have their "need-to-know" certified by the cognizant military agency of their project or contract.

Institute of Statistics
Mimeograph Series No. 300

ACKNOWLEDGEMENTS

I take great pleasure in expressing my gratitude to Professor R. C. Bose for suggesting this particular problem and for his continuing guidance and encouragement at the various stages of my research.

I wish to thank Professor R. R. Kuebler, Jr. for carefully reading the manuscript and making many excellent suggestions for improvements.

My appreciation is due to the United States Public Health Service for providing me with essential financial aid through its support of a University of North Carolina research fellowship in biostatistics. This aid would not have been possible without the assistance of Professor B. G. Greenberg, Chairman of the Department of Biostatistics, who obtained for me the appointment as fellow. I also wish to thank Professor Greenberg for his continuing interest and encouragement during the course of my graduate study.

To Miss Martha Jordan I owe a special debt of gratitude for her various forms of aid during my stay in Chapel Hill. To Mrs. Doris Gardner and Miss Martha Jordan I am extremely grateful for their skillful and quick typing of the manuscript.

Finally, I feel a deep indebtedness to Mr. L. J. Adams, Chairman of the Department of Mathematics at Santa Monica City College, for encouraging me to study mathematics in my earliest college days.

TABLE OF CONTENTS

Chapter		Page
	ACKNOWLEDGMENTS	ii
	INTRODUCTION	v
I	NECESSARY AND SUFFICIENT CONDITIONS FOR THE EXISTENCE OF BURST-ERROR-CORRECTING CODES	1
	1.1. Introduction - Necessary and Sufficient Conditions for the Existence of Error Correcting Codes	1
	1.2. Definition of Bursts of Errors. Necessary and Sufficient Conditions for the Existence of Burst-Error-Correcting Codes	5
	1.3. Some Elementary Properties of Galois Fields	7
	1.4. Efficiency of Burst-Error-Correcting Codes. The Hamming and Abramson Codes	10
II	BINARY GROUP CODES WHICH CORRECT ERRORS IN BURSTS OF LENGTH d OR LESS, $d = 3, 4 \dots$	16
	2.1. Preliminary Considerations. Codes of Bose and Chakravarti	16
	2.2. Binary Group Codes which Correct Errors in Bursts of Three or Less for Odd Redundancy	24
	2.3. Binary Group Codes which Correct Errors in Bursts of Four or Less for the following Redundancies: $r_1 = 3k_1 + 1$, $r_2 = 4k_2$, and $r_3 = 4k_3 + 3$, where $k_1 \geq 3$, $k_2 \geq 3$ and $k_3 \geq 2$	34
III	p -NARY LINEAR CODES WHICH CORRECT ERRORS IN BURSTS OF LENGTH d OR LESS, FOR $p = 3, 5$, AND $d = 2$, AND FOR $p = 3$, $d = 3$	55
	3.1. Golay Codes	55

Chapter	Page
3.2. Ternary Linear Codes which Correct Errors in Bursts of Two or Less	57
3.3. Quintary Linear Codes which Correct Errors in Bursts of Two or Less for Even Redundancy and Odd Redundancy of the Form $4m + 1$	75
3.4. Ternary Linear Codes which Correct Errors in Bursts of Three or Less for Even Redundancy	88
IV THE APPLICATION OF BOSE-CHAUDHURI CODES TO THE CONSTRUCTION OF BURST-ERROR-CORRECTING CODES	96
4.1. Introduction	96
4.2. Augmented Bose-Chaudhuri Codes which Correct Single Bursts of Errors	98
4.3. Augmented Bose-Chaudhuri Codes which Correct Multiple Bursts of Errors	114
4.4. Further Problems in the Construction of Multiple-Burst-Error-Correcting Codes	123
BIBLIOGRAPHY	125

INTRODUCTION

When transmitting information from one point (the source of input) to another point (the receiver or output) by some mechanical means (the channel) there is a positive probability that the received information will differ from the information transmitted.

We shall define a piece of information that is transmitted across a channel as a message. We shall require that each message is composed of symbols so that the channel actually transmits the message symbol by symbol. Thus the received message will differ from the transmitted message if any one (or more) of the symbols in the transmitted message is received incorrectly, i.e., is received as another symbol. We shall then say that an error has occurred in the transmission of a message if one of the symbols in the message is received as another symbol after transmission.

In the transmission of messages across a channel, errors often tend to occur in bursts, usually due to the presence of some disturbance in the channel for a short time, as in the case of static. That is, we may have a single "burst" of, say, two or three errors somewhere in the message whereas the remainder of the message is error-free.

We construct codes in this thesis such that if a message of the code is received containing a burst of errors, it will still be decoded as the correct message. In using these codes it will be necessary to add redundancy to the messages of the codes. That is, we will have to add places to the original message that do not give

any added information. These places are called check places. Thus the redundancy of a code is the price we must pay for sending a correct message. The question is then how do we obtain codes which have a minimum amount of redundancy for a given message length and which still insure that although a transmitted message may contain a burst of errors of a given length, it will be decoded as the correct message.

In Chapter I we derive the necessary and sufficient conditions for the existence of single-burst-error-correcting codes in general, and survey the past work which has been done in constructing burst-error-correcting codes which are binary. (Binary codes are codes whose symbols are zeros and ones.) The most notable work was done by Abramson [1]¹. However, he considered only the construction of a certain class of binary codes, called binary group codes, which correct single bursts of errors of length two or less. We also discuss briefly some of the elementary properties of Galois fields, since we use Galois fields exclusively to construct the codes in this thesis.

In Chapter II we construct group codes for the binary case which correct single bursts of errors of length three or less when the redundancy is odd, and some group codes which correct bursts of errors of length four or less. We introduce in this chapter the methods of cycles which we use to construct the new "3-burst"

1

The numbers in square brackets refer to the bibliography listed at the end.

error-correcting codes and one class of "4-burst" error-correcting codes. Bose and Chakravarti [5] have constructed binary group codes which correct bursts of errors of length three or less when the redundancy is even.

In Chapter III we construct ternary codes which correct single bursts of errors of length two or less when the redundancy is odd, and quintary codes which correct single bursts of errors of length two or less when the redundancy is even and when the redundancy is odd and of the form $4k + 1$. We also construct ternary codes which correct single bursts of errors of length three or less when the redundancy is even. Elspas [8] has constructed the ternary codes which correct single bursts of errors of length two or less when the redundancy is even. Again the method of construction of the codes appearing in this chapter depends on the method of cycles. We should mention that all the codes in this chapter are in a certain class of codes called linear codes.

In Chapter IV we briefly discuss some of the extensions of the codes introduced by Bose and Chaudhuri [6] to correcting more than one burst of errors or multiple burst of errors that may occur in a message.

CHAPTER I

NECESSARY AND SUFFICIENT CONDITIONS FOR THE EXISTENCE OF BURST-ERROR-CORRECTING CODES

1.1 Introduction - Necessary and Sufficient Conditions for the Existence of Error-Correcting Codes.

Consider a channel which can transmit any one of s distinct symbols. We call this channel an s -ary channel. Due to the presence of "noise", a transmitted symbol may be received as one of the other $s-1$ symbols. When this occurs we say there is an error in transmission. We shall restrict s to be the power of a prime number, so that there exists a Galois field $GF(s)$ whose elements can be identified with the s symbols that can be transmitted.

We consider n -place messages as n -place vectors each of whose elements is an element of $GF(s)$ (i.e., $\alpha = (a_1, \dots, a_n)$ is an n -place message, where $a_i \in GF(s)$). Let B_n be the set of all n -vectors whose elements belong to $GF(s)$. Then B_n is a vector space. The number of elements in B_n is s^n . We shall call the message presented to the channel the input and the message received the output. We shall assume throughout this thesis that the message lengths of inputs and outputs are the same.

If $\alpha = (a_1, \dots, a_n)$ is the input message and $\alpha^* = (b_1, \dots, b_n)$ is the output message, where a_i and b_i are in $GF(s)$ for all i , we say that $\epsilon = \alpha^* - \alpha$ is the error or "noise" vector. Thus, letting $\epsilon = (\epsilon_1, \dots, \epsilon_n)$, we say there is an error in the i -th place of the received message α^* if and only if $\epsilon_i \neq 0$.

Let Γ be a subset of the s^n error vectors which we want to correct with certainty, and let us choose a subset \mathcal{Q} of inputs as our set of messages - the number of elements in \mathcal{Q} being $v < s^n$. Let $\alpha_0, \alpha_1, \dots, \alpha_{v-1}$ denote the inputs, i.e., elements of \mathcal{Q} . We divide the vectors of B_n into disjoint subsets S_0, \dots, S_{v-1} , where $\alpha_i \in S_i$. We now make the following rule: if the output belongs to the set S_i , we read the message as α_i , so that there is a one-one correspondence between the subsets of B_n and the input messages which constitute the code \mathcal{Q} . The rule is called the decoding scheme or the decoder. If $\alpha_i \in \mathcal{Q}$ is the input and if the output α_i^* also belongs to S_i , we get the correct message α_i .

Definition 1.1.1. \mathcal{Q} - the subset of inputs - is called a group code if the elements of \mathcal{Q} form a group under vector addition.

\mathcal{Q} is called a linear code if the elements of \mathcal{Q} form a vector space.

We shall consider only linear codes in this thesis.

If k is the rank of \mathcal{Q} , then the number of elements in \mathcal{Q} is s^k . Now set $n = k + r$; then r is called the redundancy of the code. The redundancy is the price we must pay for sending correct messages.

Definition 1.1.2. We say that two error vectors ϵ_1 and ϵ_2 are aliases of one another if $\epsilon_1 - \epsilon_2$ belongs to \mathcal{Q} - the set of messages.

Suppose the vectors $\alpha_0, \dots, \alpha_{k-1}$ form a basis for \mathcal{Q} . Then the aliases of the error vector ϵ are $\epsilon + \sum_{i=0}^{k-1} c_i \alpha_i$ where $c_i \in GF(s)$ for

$i = 0, \dots, k-1$. Thus each alias set contains s^k vectors, and the totality of s^n error vectors is divisible into s^r disjoint alias sets.

We can now describe an error-correcting code. Let the error vectors belonging to $\underline{[]}$ be $\epsilon_0, \epsilon_1, \dots, \epsilon_{u-1}$ where $u \leq s^r$. If we choose \mathcal{Q} such that no two of $\epsilon_0, \epsilon_1, \dots, \epsilon_{u-1}$ belong to the same alias set, then there exists a decoding rule which corrects with certainty the errors belonging to $\underline{[]}$. Under the stated condition, for $0 \leq j \leq u-1$, there is one and only one alias set containing ϵ_j . Let us call this set \mathcal{Q}_j . Choose $\epsilon_u, \epsilon_{u+1}, \dots, \epsilon_{s^r-1}$ so that they belong one each to the s^r-u alias sets other than $\mathcal{Q}_0, \mathcal{Q}_1, \dots, \mathcal{Q}_{u-1}$. Then define the subset S_j corresponding to α_j as the set whose elements are $\alpha_j + \epsilon_0, \alpha_j + \epsilon_1, \dots, \alpha_j + \epsilon_{u-1}, \alpha_j + \epsilon_u, \dots, \alpha_j + \epsilon_{s^r-1}$. Thus, if any error belonging to $\underline{[]}$ or to the set $\{\epsilon_u, \epsilon_{u+1}, \dots, \epsilon_{s^r-1}\}$ has occurred, it follows that the error will be corrected with certainty.

Let the vector space \mathcal{Q} (the set of messages) be generated by $\alpha_0, \alpha_1, \dots, \alpha_{k-1}$, and let

$$(1.1) \quad A = A(k \times n) = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \end{bmatrix} .$$

Clearly, $\text{rank}(A) = k$. Now let $\overline{\mathcal{Q}}$ be the vector space generated by all column vectors

$$\underline{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

for which $A\underline{x} = \underline{0}$; i.e., $\bar{\mathcal{Q}}$ is the vector space orthogonal to \mathcal{Q} . Then $\bar{\mathcal{Q}}$ has rank $r = n-k$. We now make the following definition.

Definition 1.1.3. Let D be an $n \times r$ matrix whose column vectors generate $\bar{\mathcal{Q}}$. Then D is called a parity check matrix of the code.

Thus, a vector $\alpha = (a_1, \dots, a_n)$ belongs to \mathcal{Q} if and only if $\alpha D = \underline{0}'$. We now can formulate the following theorem.

Theorem 1.1.1. A necessary and sufficient condition for any two error vectors ϵ_i and ϵ_j , $i \neq j$, to belong to the same alias set is $(\epsilon_i - \epsilon_j)D = \underline{0}'$.

Proof. Suppose that ϵ_i and ϵ_j belong to the same alias set. Then, by Definition 1.1.2, $\epsilon_i - \epsilon_j$ belongs to \mathcal{Q} - the set of messages. Hence, $(\epsilon_i - \epsilon_j)D = \underline{0}'$.

Suppose $(\epsilon_i - \epsilon_j)D = \underline{0}'$. Then, by Definition 1.1.3, $\epsilon_i - \epsilon_j$ belongs to $\bar{\mathcal{Q}}$, and hence, by Definition 1.1.2, ϵ_i and ϵ_j are in the same alias set.

Corollary 1.1.1. Suppose $\underline{(\quad)}$ is the set of error vectors $\epsilon_0, \dots, \epsilon_{u-1}$. Then in order to obtain a code \mathcal{Q} for which errors belonging to $\underline{(\quad)}$ will be corrected with certainty, it is sufficient to obtain a parity check matrix D such that the row vectors $\epsilon_0 D, \dots, \epsilon_{u-1} D$ are all distinct.

Proof. The condition that no alias set contain more than one element of $\underline{(\quad)}$ is, by Theorem 1.1.1, equivalent to the condition that

$\epsilon_0^D, \dots, \epsilon_{u-1}^D$ are all distinct.

1.2. Definition of Bursts of Errors. Necessary and Sufficient Conditions for the Existence of Burst-Error-Correcting Codes.

Gilbert, reference [9], defines an error burst of length d for binary codes. We give here the analogous definition for s -ary codes.

Definition 1.2.1. For any s -ary code we define a burst sequence of length d as any sequence of symbols (from $GF(s)$) of length d beginning and ending with non-zero symbols. The number of such sequences is $s^{d-2}(s-1)^2$. Consider now an error vector $\epsilon = (\epsilon_1, \dots, \epsilon_n)$. If $\epsilon_i, \epsilon_{i+1}, \dots, \epsilon_{i+d-1}$, $i \geq 0$, where the subscripts have been reduced mod n , is a burst sequence, and if all other elements of ϵ are zero, then ϵ is said to be an error vector with a single burst of length d .

For examples of error vectors with a single burst of length d , let us consider the case $d = 3$, $n = 7$, and $s = 2$. Then the error vectors of length 7 which contain a single binary burst of length 3 are: (1110000), (0111000), (0011100), (0001110), (0000111), (1000011), (1100001), (1010000), (0101000), (0010100), (0001010), (0000101), (1000010), (0100001). Suppose $d = 2$, $n = 5$, and $s = 3$. Then the error vectors of length 5 which contain a single ternary burst of length 2 are: (11000), (12000), (21000), (22000), (01100), (01200), (02100), (02200), (00110), (00120), (00210), (00220), (00011), (00012), (00021), (00022), (10001), (20001), (10002), (20002).

In construction of burst-error-correcting codes we will require that the codes correct not only single bursts of length d but also all single bursts of length less than d . For example, if $d = 3$ and $s = 2$ we will require the code to correct all error vectors containing single burst sequences of the form 1, 11 as well as those of the form 101 and 111. Thus, in general our error set \underline{E} will contain

$$(1.2) \quad n \sum_{e=2}^d s^{e-2}(s-1)^2 + n(s-1)$$

vectors, provided $n > 2d$. (1.2) is easily evaluated, and we have

$$(1.3) \quad n \sum_{e=2}^d s^{e-2}(s-1)^2 + n(s-1) = ns^{d-1}(s-1) \quad .$$

We now formulate Theorem 1.2.1.

Theorem 1.2.1. Let \underline{E} be the error set which contains all $ns^{d-1}(s-1)$ burst error vectors of length less than or equal to d . Then in order to obtain a code for which errors belonging to \underline{E} will be corrected with certainty, it is necessary and sufficient to obtain a parity check matrix $D = D(n \times r)$ such that the row vectors $\{\epsilon_j D\}$, $j=0, 1, \dots, ns^{d-1}(s-1) - 1$, $\epsilon_j \in \underline{E}$, are all distinct.

The proof follows from Corollary 1.1.1.

Example 1.2.1. Suppose $s = 2$ and $d = 3$; then, by Theorem 1.2.1, finding a code for which the error vectors which contain single burst sequences of the form 1, 11, 101, 111 will be corrected with certainty is equivalent to finding a parity check matrix D where

$$(1.4) \quad D = \begin{bmatrix} \delta_0 \\ \delta_1 \\ \vdots \\ \delta_{n-1} \end{bmatrix}$$

such that δ_i , $\delta_i + \delta_{i+1}$, $\delta_i + \delta_{i+2}$, and $\delta_i + \delta_{i+1} + \delta_{i+2}$, $i = 0, 1, \dots, n-1$, are all distinct. (Note. We reduce the subscripts of these vectors mod n so that we can correct all bursts included in Definition 1.2.1.)

Example 1.2.2. Suppose $s = 3$ and $d = 2$; then again by Theorem 1.2.1 it is necessary and sufficient to obtain a parity check matrix D as given in (1.4) such that δ_i , $2\delta_i$, $\delta_i + \delta_{i+1}$, $\delta_i + 2\delta_{i+1}$, $2\delta_i + \delta_{i+1}$, and $2\delta_i + 2\delta_{i+1}$, $i = 0, 1, \dots, n-1$, are all distinct.

1.3. Some Elementary Properties of Galois Fields.

Since the construction of the burst-error-correcting codes in this thesis is done by use of Galois fields, we discuss briefly in this section some of the elementary properties of Galois fields. For a more complete discussion of the subject, reference [7], pp. 242-288, or [3], pp. 427-456, should be consulted.

Definition 1.3.1. A Galois field $GF(p^m)$ is a finite field with characteristic p , where p is a prime.

We state without proof the essential properties of Galois fields we will need.

(i) In each Galois field $GF(p^m)$ there are elements x called primitive elements of $GF(p^m)$, then x^0, x, \dots, x^{p^m-2} are all ^{the} distinct

non-zero elements of the field.

(ii) Suppose $a_0 + a_1x + \dots + a_mx^m$ is an irreducible polynomial of degree m over $GF(p)$ which divides $x^{p^m-1} - 1$ and does not divide $x^t - 1$ for $t < p^m - 1$. The roots of

$$(1.5) \quad a_0 + a_1x + \dots + a_mx^m = 0$$

are primitive elements of $GF(p^m)$, and the left-hand member of (1.5) is called the characteristic polynomial.

(iii) We can associate each non-zero element of $GF(p^m)$ with the m -place non-zero vector $(c_0, c_1, \dots, c_{m-1})$ each of whose coordinates belongs to $GF(p)$. This is done as follows. We can rewrite (1.5) as

$$x^m = b_0 + b_1x + \dots + b_{m-1}x^{m-1}$$

since $a_m \neq 0$. By making use of this relation we can express any x^i ($0 \leq i \leq p^m - 2$) as an $(m-1)$ -th degree or lesser degree polynomial in x :

$$x^i = c_0 + c_1x + \dots + c_{m-1}x^{m-1},$$

where $c_j \in GF(p)$. Then the coefficient vector (c_0, \dots, c_{m-1}) is associated with x^i . In this way all the distinct $p^m - 1$ non-zero vectors are associated with the distinct non-zero elements of the field.

(iv) If x is a primitive element of $GF(p^m)$ satisfying (1.5), and if τ and $p^m - 1$ are relatively prime, $x' = x^\tau$ is also a primitive element of $GF(p^m)$ satisfying some characteristic polynomial equation

$$(1.6) \quad a'_0 + a'_1x + \dots + a'_mx^m = 0,$$

where again $a_i \in \text{GF}(p)$ for $i = 0, 1, \dots, m$. If τ is of the form p^k , $k = 0, 1, \dots, m-1$, then the left-hand members of (1.5) and (1.6) are the same characteristic polynomial.

For an example of a Galois field, consider $p = 2$ and $m = 4$. Then the roots of $1 + x + x^4 = 0$ are primitive elements of $\text{GF}(2^4)$. Using the above characteristic polynomial we can represent the distinct non-zero elements of $\text{GF}(2^4)$ as the fifteen four-place non-zero vectors over $\text{GF}(2)$ as follows:

Table I

x^0	$= 1$	$= (1000)$
x^1	$= x$	$= (0100)$
x^2	$= x^2$	$= (0010)$
x^3	$= x^3$	$= (0001)$
x^4	$= 1 + x$	$= (1100)$
x^5	$= x + x^2$	$= (0110)$
x^6	$= x^2 + x^3$	$= (0011)$
x^7	$= 1 + x + x^3$	$= (1101)$
x^8	$= 1 + x^2$	$= (1010)$
x^9	$= x + x^3$	$= (0101)$
x^{10}	$= 1 + x + x^2$	$= (1110)$
x^{11}	$= x + x^2 + x^3$	$= (0111)$
x^{12}	$= 1 + x + x^2 + x^3$	$= (1111)$
x^{13}	$= 1 + x^2 + x^3$	$= (1011)$
x^{14}	$= 1 + x^3$	$= (1001)$

1.4. Efficiency of Burst-Error-Correcting-Codes. The Hamming and Abramson Codes.

Let $D = D(n \times r)$ be a parity check matrix for the s -ary code which corrects all bursts of errors less than or equal to d in length. We shall derive an upper bound for n - the total number of message places for the code corresponding to D with a fixed redundancy r . Let $\delta_0, \delta_1, \dots, \delta_{n-1}$ be the $1 \times r$ row vectors of D . Then each row vector $\delta_i = (d_{i1}, \dots, d_{ir})$, $i = 0, 1, \dots, n-1$, is a non-null row vector each of whose coordinates d_{ij} , $j = 1, \dots, r$, belongs to $GF(s)$. Thus, the maximum number of row vectors in D is $s^r - 1$. Since D is the parity check matrix for the s -ary code which corrects all bursts of length less than or equal to d , we have by (1.3) that the number of distinct vectors of the form $\epsilon_j D$ is $n s^{d-1}(s-1)$, where $\epsilon_j \in \underline{(\quad)}$ - the set of errors to be correct with certainty. These vectors are also $1 \times r$ row vectors whose coordinates are in $GF(s)$ and thus

$$s^r - 1 \geq n s^{d-1}(s-1)$$

or

$$(1.7) \quad \frac{s^r - 1}{s^{d-1}(s-1)} \geq n$$

We have thus proved that the maximum number of message places for the s -ary linear code which for a fixed redundancy corrects all bursts of errors of length less than or equal to d is

Then $D_{1,m}$ is a parity check matrix for the binary group¹ code which corrects all single errors, where $n = 2^m - 1$ and $r = m$. To prove $D_{1,m}$ has the required property it suffices to show that $\delta_0, \dots, \delta_{2^m-2}$ are all distinct, where δ_i is the coefficient vector of the $(m-1)$ -th degree polynomial in x which represents x^i . If two vectors, say δ_j and δ_k , were identical $k \neq j$ and $0 \leq j, k \leq 2^m - 2$, this would imply $x^j = x^k$, which would in turn imply that $x^{j-k} = 1$ where $j - k < 2^m - 1$. This, however, would contradict the fact that x is a primitive element of $GF(2^m)$. Thus $D_{1,m}$ is a parity check matrix for the binary group code which corrects all single errors, where $n = 2^m - 1$ and $r = m$. The corresponding codes are called Hamming codes since they were discovered by Hamming [11] in 1950. These codes, in accordance with Definition 1.4.1, have efficiency 1, or maximum efficiency, for

$$n = 2^m - 1$$

and

$$n_0 = \left[\frac{2^m - 1}{1} \right] = 2^m - 1,$$

whence $n/n_0 = 1$.

For an example of a Hamming code, let $m = 4$, then x is a primitive element of $GF(2^4)$, where we take $x^4 + x + 1$ as the characteristic polynomial which has x as one of its roots. A parity check matrix for this code is then $D_{1,4}$, where

1. Groups codes and linear codes are equivalent for the binary case.

$$D_{1,4} = \begin{bmatrix} 1 \\ x \\ x^2 \\ \vdots \\ x^{14} \end{bmatrix}$$

and where x^i ($i = 0, 1, \dots, 14$) stands for the vector corresponding to x^i in Table I. Thus, the code corresponding to $D_{1,4}$ is a 15-place binary group code, with 4 redundancy places, which corrects all single errors occurring in transmission.

Again let x be a primitive element of $GF(2^m)$ and now consider the matrix

$$D_{2,m} = \begin{bmatrix} 1 & 1 \\ x & 1 \\ x^2 & 1 \\ \vdots & \vdots \\ x^{2^m-2} & 1 \end{bmatrix} \begin{matrix} \delta_0 \\ \delta_1 \\ \delta_2 \\ \vdots \\ \delta_{2^m-2} \end{matrix}$$

Then $D_{2,m}$ is a parity check matrix for the binary group code which corrects all single errors and all double adjacent errors, where $n = 2^m - 1$ and $r = m + 1$. To show that $D_{2,m}$ has the required property, we must show that the vectors $\delta_0, \delta_1, \dots, \delta_{n-1}, \delta_0 + \delta_1, \delta_1 + \delta_2, \dots, \delta_{n-1} + \delta_0$ are all distinct, where δ_i represents the $(m+1)$ -place vector in which the first m places are filled by the coefficients of the polynomial represented by x^i and the last place is filled by a 1.

Now, clearly $\delta_0, \dots, \delta_{n-1}$ are distinct among themselves. Next, $\delta_i + \delta_{i+1} = (x^i, 1) + (x^{i+1}, 1) = (x^i(1+x), 0)$. Now let $1+x = x^0$; then $\delta_i + \delta_{i+1} = (x^{i+0}, 0)$ and hence, for $i = 0, 1, \dots, 2^m - 2$, the vectors $\delta_i + \delta_{i+1}$ are distinct among themselves. Finally, for any j , $0 \leq j \leq 2^m - 2$, and any k , $0 \leq k \leq 2^m - 2$, $\delta_j \neq \delta_k + \delta_{k+1}$ since the last place of δ_j is filled by a 1 and the last place of $\delta_k + \delta_{k+1}$ is filled by a 0. Thus, $D_{2,m}$ is a parity check matrix for the binary group code which corrects all single errors and all double adjacent errors, where $n = 2^m - 1$, and $r = m + 1$. The corresponding codes are known as single-error-or-double-adjacent-error-correcting-codes. These codes were discovered by Abramson [1] in 1959. Again as with the Hamming codes, these codes have maximum efficiency in the sense of Definition 1.4.1. Here,

$$n = 2^m - 1$$

and

$$n_0 = \left[\frac{2^{m+1} - 1}{2} \right] = 2^m - 1.$$

Thus, $n/n_0 = 1$.

For an example of a single-error-or-double-adjacent-error-correcting code, suppose $m = 4$, and let x be a primitive element of $GF(2^4)$, satisfying the characteristic polynomial equation $x^4 + x + 1 = 0$. Then the parity check matrix of the binary group code which has 15 message places, with 4 redundancy places, is:

$$D_{2,4} = \begin{bmatrix} 1 & 1 \\ x & 1 \\ x^2 & 1 \\ \vdots & \vdots \\ x^{14} & 1 \end{bmatrix}$$

where x^i ($i = 0, 1, \dots, 14$) stands for the vector corresponding to x^i in Table I.

Thus, the problem of constructing binary group codes with maximum efficiency that correct single errors and errors which occur in bursts of two or less has a known solution. In Chapter II, methods are given for constructing binary group codes which correct errors occurring in bursts of 3 or less and in bursts of 4 or less.

CHAPTER II

BINARY GROUP CODES WHICH CORRECT ERRORS IN BURSTS OF LENGTH

d OR LESS, $d = 3, 4$

2.1. Preliminary Considerations. Codes of Bose and Chakravarti.

Bose and Chakravarti [5] have constructed parity check matrices for binary group codes which correct errors in bursts of three or less when the redundancy of the code is even. They showed that these matrices give codes which have maximum efficiency in accordance with Definition 1.4.1. We discuss this method here, as the techniques used in the construction of the Bose-Chakravarti codes are generalized to the construction of the new codes that appear in this chapter.

Suppose that $r = m + 2$ where $m \geq 4$ is even, and suppose that y is a primitive element of $GF(2^m)$. Suppose, further, that z is a primitive element of $GF(2^2)$, which is a subfield of $GF(2^m)$ since m is even. We now consider the matrix $D_{3,m+2}$, where

$$D_{3,m+2} = \begin{array}{|c|c|} \hline 1 & 1 \\ y & z \\ y^2 & z^2 \\ \hline y^3 & 1 \\ y^4 & z \\ y^5 & z^2 \\ \hline \vdots & \vdots \\ \hline y^{2^m-4} & 1 \\ y^{2^m-3} & z \\ y^{2^m-2} & z^2 \\ \hline \end{array}$$

We should remember that y^i is equivalent to the m -vector with elements from $GF(2)$ which is the coefficient vector of the $(m-1)$ -th degree polynomial in y representing y^i . Similarly, z^i (where i is taken mod 3) is equivalent to the 2-vector with elements from $GF(2)$ which is the coefficient vector of the first degree polynomial in z representing z^i . Thus $D_{3,m+2} = D_{3,m+2} \left[(2^m - 1) \times (m + 2) \right]$. In order that $D_{3,m+2}$ be an appropriate parity check matrix for the binary group code which corrects errors in bursts of three or less, the vectors in the following sets must all be distinct (see Theorem 1.2.1).

$$(2.1) \quad \epsilon_{i1} D_{3,m+2}, \epsilon_{i2} D_{3,m+2}, \epsilon_{i3} D_{3,m+2}, \epsilon_{i4} D_{3,m+2},$$

for $i = 1, 2, \dots, 2^{m-1}$, and

$$\begin{array}{c}
 * \\
 \downarrow \\
 \epsilon_{i1} = (0, 0, \dots, 0, 1, 0, \dots, 0, 0) \quad , \\
 * \\
 \downarrow \\
 \epsilon_{i2} = (0, 0, \dots, 0, 1, 1, 0, \dots, 0, 0) \quad , \\
 * \\
 \downarrow \\
 \epsilon_{i3} = (0, 0, \dots, 0, 1, 0, 1, 0, \dots, 0, 0) \quad , \\
 * \\
 \downarrow \\
 \epsilon_{i4} = (0, 0, \dots, 0, 1, 1, 1, 0, \dots, 0, 0) \quad ,
 \end{array}$$

where the star indicates the i -th position in ϵ_{ij} , $j = 1, 2, 3, 4$.
 Performing the required multiplications in (2.1), we obtain the following sets of vectors:

$$(2.2) \quad \delta_i = \begin{bmatrix} y^i \\ z^i \end{bmatrix}, \quad i = 0, 1, \dots, 2^m - 2,$$

$$(2.3) \quad \delta_i + \delta_{i+1} = \begin{bmatrix} y^i(1+y) \\ z^i(1+z) \end{bmatrix}, \quad i = 0, 1, \dots, 2^m - 2;$$

$$(2.4) \quad \delta_i + \delta_{i+2} = \begin{bmatrix} y^i(1+y^2) \\ z^i(1+z^2) \end{bmatrix}, \quad i = 0, 1, \dots, 2^m - 2;$$

$$(2.5) \quad \delta_i + \delta_{i+1} + \delta_{i+2} = \begin{bmatrix} y^i(1+y+y^2) \\ z^i(1+z+z^2) \end{bmatrix}, i = 0, 1, \dots, 2^m - 2.$$

Thus, $D_{3,m+2}$ is an appropriate parity check matrix for the binary group code, with $n = 2^m - 1$ and $r = m + 2$ (m even), which corrects all single error bursts of length 3 or less if the vectors in (2.2), (2.3), (2.4) and (2.5) are all distinct. We shall say that the matrix $D_{3,m+2}$ possesses the property B_3 if the vectors in (2.2)-(2.5)

are all distinct. Thus, the property B_3 is necessary and sufficient for $D_{3,m+2}$ to be a parity check matrix for a binary group code correcting all error vectors which contain a single burst of length 3 or less. [Similarly, we shall say that $D_{3,2m+1}$ possesses property B_3 , where $D_{3,2m+1}$ is defined in the next section.]

Theorem 2.1.1. Suppose we let $1 + y = y^\theta$, and $1 + y + y^2 = y^\phi$. Then a necessary and sufficient condition that $D_{3,m+2}$ have property B_3 is that $\theta \neq 2 \pmod{3}$.

Proof. First of all, since z is a primitive element of $GF(2^2)$, $1 + z = z^2$, $1 + z^2 = z$, and $1 + z + z^2 = 0$. Thus (2.2), (2.3), (2.4) and (2.5) become:

$$(2.2') \quad \delta_i = \left(y^i, z^i \right), \quad i = 0, 1, \dots, 2^m - 2;$$

$$(2.3') \quad \delta_i + \delta_{i+1} = \left(y^{i+\theta}, z^{i+2} \right), \quad i = 0, 1, \dots, 2^m - 2;$$

$$(2.4') \quad \delta_i + \delta_{i+2} = \left(y^{i+2\theta}, z^{i+1} \right), \quad i = 0, 1, \dots, 2^m - 2;$$

$$(2.5') \quad \delta_i + \delta_{i+1} + \delta_{i+2} = \left(y^{i+\phi}, 0 \right), \quad i = 0, 1, \dots, 2^m - 2.$$

It is clear that these vectors are distinct within each set; for example, in (2.2') the elements $1, y, \dots, y^{2^m-2}$ are all the distinct non-zero elements of $GF(2^m)$. Hence, the only possible way in which condition B_3 could be violated is that two vectors, chosen one each from two different sets (2.2'), (2.3'), (2.4'), and (2.5'), be equal. Suppose now that the i -th vector from (2.2') were equal to the j -th vector of (2.3'), that is, $\delta_i = \delta_j + \delta_{j+1}$. Then the following equations must hold simultaneously:

$$\begin{aligned} y^i &= y^{j+\theta} \quad , \\ z^i &= z^{j+2} \quad ; \end{aligned}$$

that is,

$$\begin{aligned} i - j &= \theta \quad , \\ i - j &= 2 \pmod{3} \end{aligned}$$

must hold together. This will happen if and only if $\theta = 2 \pmod{3}$. Similarly we can show that the only way in which the i -th vector from the set (2.2') can equal the k -th vector from the set (2.4') is that $\theta = 2 \pmod{3}$, and that this is also the necessary and sufficient condition for the j -th vector of the set (2.3') to equal the k -th vector of the set (2.4'). Finally, we note that the elements of the set of vectors (2.5') are distinct from the elements of the sets of vectors (2.2'), (2.3'), and (2.4') since the last position of each vector in (2.5') contains a zero whereas the last position of each vector in the other sets contains a non-zero element. This completes the proof.

If y is a primitive element of $GF(2^m)$ such that $\theta = 2 \pmod{3}$, it is a conjecture that it is always possible to find another primitive element $y' = y^\tau$, where $2^m - 1$ and τ are relatively prime, such that if we set $1 + y' = y'^{\theta'}$, then $\theta' \not\equiv 2 \pmod{3}$. This technique is exhibited in Example 2.1.3.

We now prove that the binary group codes whose parity check matrices are constructed in the above manner so as to possess property B_3 have optimum efficiency as given by Definition 1.4.1. For these matrices $n = 2^m - 1$ and $r = m + 2$. Thus, by Definition 1.4.1,

$$n_0 = \left[\frac{2^{m+2} - 1}{2^2} \right] = 2^m - 1 .$$

Hence, $n/n_0 = 1$.

We now give some examples of these codes.

Example 2.1.1. Let $m = 4$, whence $n = 15$, $r = 6$. We then

have

$$D_{3,6} = \begin{bmatrix} 1 & 1 \\ y & z \\ y^2 & z^2 \\ \hline y^3 & 1 \\ y^4 & z \\ y^5 & z^2 \\ \hline y^6 & 1 \\ y^7 & z \\ y^8 & z^2 \\ \hline y^9 & 1 \\ y^{10} & z \\ y^{11} & z^2 \\ \hline y^{12} & 1 \\ y^{13} & z \\ y^{14} & z^2 \end{bmatrix} = \begin{bmatrix} 1000 & 10 \\ 0100 & 01 \\ 0010 & 11 \\ \hline 0001 & 10 \\ 1100 & 01 \\ 0110 & 11 \\ \hline 0011 & 10 \\ 1101 & 01 \\ 1010 & 11 \\ \hline 0101 & 10 \\ 1110 & 01 \\ 0111 & 11 \\ \hline 1111 & 10 \\ 1011 & 01 \\ 1001 & 11 \end{bmatrix}$$

Since the characteristic polynomial for $GF(2^4)$ is $y^4 + y + 1$, we

have $1 + y = y^4$, so that $\theta = 4 \not\equiv 2 \pmod{3}$. It then follows from Theorem 2.1.1 that $D_{3,6}$ possesses property B_3 . Hence, $D_{3,6}$ is a parity check matrix for the binary group code which has 15 message places and 6 redundancy places and which corrects errors occurring in bursts of 3 or less.

Example 2.1.2. Let $m = 6$. Then $n = 63$ and $r = 8$. Thus we have:

$$D_{3,8} = \begin{bmatrix} 1 & 1 \\ y & z \\ y^2 & z^2 \\ \hline y^3 & 1 \\ y^4 & z \\ y^5 & z^2 \\ \hline \vdots & \vdots \\ \hline y^{60} & 1 \\ y^{61} & z \\ y^{62} & z^2 \end{bmatrix}$$

Since $1 + y + y^6$ is a characteristic polynomial for $GF(2^6)$ we can take y as a root of this polynomial and then y will be a primitive element of $GF(2^6)$. Thus we can set $y^6 = y + 1$, whence again it follows from Theorem 2.1.1 that $D_{3,8}$ possesses property B_3 . Hence, $D_{3,8}$ is a parity check matrix for the binary group code which corrects errors in single bursts of 3 or less and which has 63 message places and 8 redundancy places.

Example 2.1.3. Let $m = 10$. Then $n = 1,023$ and $r = 12$. A characteristic polynomial for $\text{GF}(2^{10})$ is $y^{10} + y^3 + 1$. Now it follows that $1 + y = y^{77}$ and thus $9 = 77 = 2 \pmod{3}$. Hence Theorem 2.1.1 is not directly helpful. Let $y' = y^5$. Then since 1,023 and 5 are relatively prime, y' is again a primitive element of $\text{GF}(2^{10})$. (See iv of Section 1.3.) Thus we can take

$$D_{3,12} = \begin{bmatrix} 1 & 1 \\ y' & z \\ y'^2 & z^2 \\ \hline y'^3 & 1 \\ y'^4 & z \\ y'^5 & z^2 \\ \hline \vdots & \vdots \\ \hline y'^{1020} & 1 \\ y'^{1021} & z \\ y'^{1022} & z^2 \end{bmatrix},$$

as the parity check matrix for our code in accordance with Theorem 2.1.1, for now we can show that $1 + y' = y'^{921}$ and $921 \not\equiv 2 \pmod{3}$.

Thus, $D_{3,12}$ is the parity check matrix for the binary group code which corrects all errors occurring in single bursts of length 3 or less and which has 1023 message places and 12 redundancy places.

2.2. Binary Group Codes Which Correct Errors in Bursts of Three or Less for Odd Redundancy

In this section we introduce the method of "cycling" in Galois fields. We shall use this method to obtain the codes in this section and also to obtain certain binary group codes which correct single bursts of errors of length 4 or less, as discussed in the next section. We shall also use the cycling method to construct the codes in the next chapter.

Definition 2.2.1. Let p be an arbitrary prime. Suppose that y is a primitive element of $GF(p^m)$ and that z is a primitive element of $GF(p^{m-\nu})$ $m > \nu$. Further, suppose that δ_1 is an integer that divides $p^m - 1$ and that δ_2 is an integer dividing $p^{m-\nu} - 1$. Consider the vectors $(y^{\delta_1 i}, z^{\delta_2 i})$ for $i = 0, 1, \dots, \ell - 1$. These vectors are said to form a cycle of length ℓ if:

(i) they are all distinct,

and

(ii) $(y^{\delta_1 \ell}, z^{\delta_2 \ell}) = (1, 1)$.

Clearly, $\ell \leq \frac{(p^m - 1)(p^{m-\nu} - 1)}{\delta_1 \delta_2}$. This follows from $y^{p^m - 1} = z^{p^{m-\nu} - 1} = 1$.

Lemma 2.2.1. Suppose that y is a primitive element of $GF(p^m)$ and that z is a primitive element of $GF(p^{m-\nu})$, $m > \nu$, as given in Definition 2.2.1. Suppose that d_1 and d_2 are divisors of $p^m - 1$ and $p^{m-\nu} - 1$, respectively, such that

$$v_1 = \frac{p^m - 1}{d_1} \quad \text{and} \quad v_2 = \frac{p^{m-v} - 1}{d_2}$$

are relatively prime. Then the vectors $(y^{d_1 i}, z^{d_2 i})$, $i = 0, 1, \dots, v_1 v_2 - 1$, form a cycle of length $v_1 v_2$.

Proof. To prove the lemma we must show that the two conditions of Definition 2.2.1 are satisfied. First of all, suppose that for $i_1 \neq i_2$ (and without loss of generality we take $i_1 > i_2$), $0 \leq i_1, i_2 \leq v_1 v_2 - 1$,

$$(y^{d_1 i_1}, z^{d_2 i_1}) = (y^{d_1 i_2}, z^{d_2 i_2}) .$$

This implies that

$$(y^{d_1(i_1-i_2)}, z^{d_2(i_1-i_2)}) = (1, 1) ,$$

or that the equations

$$(2.6) \quad \begin{aligned} y^{d_1(i_1-i_2)} &= 1 , \\ z^{d_2(i_1-i_2)} &= 1 \end{aligned}$$

hold simultaneously. Thus, from (2.6) we have that

$$\begin{aligned} d_1(i_1 - i_2) &= 0 \pmod{p^m - 1} , \\ d_2(i_1 - i_2) &= 0 \pmod{p^{m-v} - 1} \end{aligned}$$

are simultaneously satisfied. Thus v_1 divides $i_1 - i_2$ and v_2 also divides $i_1 - i_2$. Since v_1 and v_2 are relatively prime this implies that $v_1 v_2$ divides $i_1 - i_2$, which contradicts the assumption that

$0 \leq i_1, i_2 \leq v_1 v_2 - 1$ and $i_1 \neq i_2$. Hence, the vectors $(y^{d_1 i_1}, z^{d_2 i_2})$, $i = 0, 1, \dots, v_1 v_2 - 1$, are all distinct. This shows that condition (i) of Definition 2.2.1 is satisfied. Further,

$$(y^{d_1 v_1 v_2}, z^{d_2 v_1 v_2}) = (y^{(p^m - 1)v_2}, z^{(p^{m-v} - 1)v_1}) = (1, 1),$$

and so condition (ii) of Definition 2.2.1 is also satisfied and thus our proof is complete.

Lemma 2.2.2. For any $m \geq 1$, the numbers $2^m - 1$ and $2^{m-1} - 1$ are relatively prime.

Proof. If there is a common divisor $d > 1$ of $2^m - 1$ and $2^{m-1} - 1$, then we can write $2^m - 1$ as $n_1 d$ and $2^{m-1} - 1$ as $n_2 d$, with $n_1 > n_2$. But then, since $2^m - 1 = 2(2^{m-1} - 1) + 1$, we have $n_1 d = 2n_2 d + 1$, giving $d(n_1 - 2n_2) = 1$, which implies the contradiction $d \leq 1$.

Let y be a primitive element of $\text{GF}(2^m)$ and z be a primitive element of $\text{GF}(2^{m-1})$. It then follows from Lemmas 2.2.1 and 2.2.2 (with $d_1 = d_2 = 1$) that the vectors (y^i, z^i) , $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, form a cycle of length $(2^m - 1)(2^{m-1} - 1)$. We shall now consider two examples of cycles of length $(2^m - 1)(2^{m-1} - 1)$.

Example 2.2.1. Suppose that $m = 4$. Then using the characteristic polynomials $1 + y + y^4$ and $1 + z + z^3$ of $\text{GF}(2^4)$ and $\text{GF}(2^3)$, respectively, the matrix $C_4 = C_4(105 \times 7)$ is given as

$$C_4 = \begin{bmatrix} 1 & 1 \\ y & z \\ y^2 & z^2 \\ \vdots & \vdots \\ y^{14} & z^{14} \\ \hline \vdots & \vdots \\ \hline y^{90} & z^{90} \\ \vdots & \vdots \\ y^{104} & z^{104} \end{bmatrix} = \begin{bmatrix} 1000 & 100 \\ 0100 & 010 \\ 0010 & 001 \\ \vdots & \vdots \\ 1001 & 100 \\ \hline \vdots & \vdots \\ \hline 1000 & 101 \\ \vdots & \vdots \\ 1001 & 101 \end{bmatrix}$$

recalling (1) $y^{15} = z^7 = 1$, and (2) the equivalence between elements of the Galois field $GF(2^m)$ and m -vectors over $GF(2)$. C_4 represents the cycle of length 105.

Example 2.2.2. Suppose $m = 5$. Then the matrix $C_5 = C_5(465 \times 9)$ is given (with $1 + y^2 + y^5$ and $1 + z + z^4$ as characteristic polynomials in y and z) as

$$C_5 = \begin{bmatrix} 1 & 1 \\ y & z \\ \vdots & \vdots \\ y^{30} & z^{30} \\ \hline \vdots & \vdots \\ \hline y^{434} & z^{434} \\ \vdots & \vdots \\ y^{464} & z^{464} \end{bmatrix} = \begin{bmatrix} 10000 & 1000 \\ 01000 & 0100 \\ \vdots & \vdots \\ 01001 & 1000 \\ \hline \vdots & \vdots \\ \hline 10000 & 1001 \\ \vdots & \vdots \\ 01001 & 1001 \end{bmatrix}$$

Thus C_5 represents a cycle of length 465.

We now formulate the following theorem.

Theorem 2.2.1. Suppose (y^i, z^i) , $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, $m \geq 4$, form a cycle of length $(2^m - 1)(2^{m-1} - 1)$. Let θ, ϕ, τ and λ be defined as: $1 + y = y^\theta$, $1 + y + y^2 = y^\phi$, $1 + z = z^\tau$, and $1 + z + z^2 = z^\lambda$. Now let $D_{3,2m+1} = D_{3,2m+1}((2^m - 1)(2^{m-1} - 1) \times 2m + 1)$ be given as

$$D_{3,2m+1} = \begin{bmatrix} 1 & 1 & 1 \\ y & z & w \\ y^2 & z^2 & w^2 \\ \vdots & \vdots & \vdots \\ y^\ell & z^\ell & w^\ell \end{bmatrix},$$

where $\ell = (2^m - 1)(2^{m-1} - 1) - 1$, w is a primitive element of $GF(2^2)$, and the elements y^i, z^i, w^i can be reduced by use of the

relations $y^{2^m-1} = z^{2^{m-1}-1} = w^3 = 1$. (1) If m is even, a necessary

and sufficient condition that $D_{3,2m+1}$ have property B_3 is that $\theta \not\equiv 2 \pmod{3}$; and (2) if m is odd, a necessary and sufficient condition that $D_{3,2m+1}$ have property B_3 is that $\tau \not\equiv 2 \pmod{3}$.

Proof. Suppose first that m is even. Let us now define δ_i as

$$\delta_i = (y^i, z^i, w^i)$$

for $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$. First, the elements of the vector set $\{\delta_i\}$, $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, are all distinct, because (y^i, z^i) , $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, form a cycle of length $(2^m - 1)(2^{m-1} - 1)$. Next, consider the vectors

$$\delta_i + \delta_{i+1} = (y^{i+0}, z^{i+\tau}, w^{i+2})$$

for $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$. The elements of this vector set are all distinct, for if

$$\delta_{i_1} + \delta_{i_1+1} = \delta_{i_2} + \delta_{i_2+1}$$

for $i_1 \neq i_2$, $0 \leq i_1, i_2 \leq (2^m - 1)(2^{m-1} - 1) - 1$, then the equations

$$y_1^{i_1+0} = y_2^{i_2+0},$$

$$z_1^{i_1+\tau} = z_2^{i_2+\tau},$$

$$w_1^{i_1+2} = w_2^{i_2+2},$$

must hold simultaneously, which implies that

$$y_1^{i_1} = y_2^{i_2},$$

$$z_1^{i_1} = z_2^{i_2},$$

hold simultaneously, contradicting that (y^i, z^i) , $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, form a cycle of length $(2^m - 1)(2^{m-1} - 1)$.

Similarly, the elements of the vector set $\{\delta_i + \delta_{i+2}\}$, $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, are all distinct, and the elements of the vector set $\{\delta_i + \delta_{i+1} + \delta_{i+2}\}$, $i = 0, 1, \dots, (2^m - 1)(2^{m-1} - 1) - 1$, are all distinct. Now, if $\delta_i = \delta_j + \delta_{j+1}$ for some i and j , $i \neq j$, then the equations

$$y^i = y^{j+\theta} \quad ,$$

$$z^i = z^{j+\tau} \quad ,$$

$$w^i = w^{j+2} \quad ,$$

hold simultaneously. Since m is even, implying that $\text{GF}(2^2)$ is a subfield of $\text{GF}(2^m)$, it then follows that

$$i = j = \theta \quad ,$$

$$i - j = 2 \pmod{3} \quad ,$$

hold together. This is possible if and only if $\theta = 2 \pmod{3}$.

Similarly, the i -th element of the vector set $\{\delta_i\}$ will equal the j -th element of $\{\delta_i + \delta_{i+2}\}$ if and only if $\theta = 2 \pmod{3}$, and the

j -th element of the vector set $\{\delta_i + \delta_{i+1}\}$ will equal the k -th element of the vector set $\{\delta_i + \delta_{i+2}\}$ if and only if $\theta = 2 \pmod{3}$.

Finally, the elements of vector set $\{\delta_i + \delta_{i+1} + \delta_{i+2}\}$ are all distinct from the elements of the other vector sets since each element of this set contains a zero in its last position while the elements of the other vector sets contain non-zero quantities in this last position. Thus, a necessary and sufficient condition that $D_{3,2m+1}$ possess property B_3 is $\theta \neq 2 \pmod{3}$. When m is odd, $m - 1$ is even, and an argument completely analogous to the foregoing establishes $\tau \neq 2 \pmod{3}$ as a necessary and sufficient condition that $D_{3,2m+1}$ possess property B_3 .

We now discuss the efficiency of these codes. For the case with even redundancy we showed earlier that the binary group codes whose parity check matrices possess property B_3 have maximum efficiency. For the odd redundancy cases the efficiency will not be maximum.

Theorem 2.2.2. Let the efficiency of the code corresponding to $D_{3,2m+1}$ be given as a_m . Then

$$(i) \quad a_m = \frac{(2^m - 1)(2^{m-1} - 1)}{2^{2m-1} - 1} \quad ;$$

(ii) $a_{m+1} > a_m$, i.e., a_m is a strictly increasing function of the integer m ; and

$$(iii) \quad \lim_{m \rightarrow \infty} a_m = 1.$$

Proof. (i) By Definition 1.4.1, $a_m = n/n_0$ where $n = (2^m - 1) \cdot (2^{m-1} - 1)$ and

$$n_0 = \left[\frac{2^{2m+1} - 1}{2^2} \right] = 2^{2m-1} - 1 \quad .$$

Thus,

$$a_m = \frac{(2^m - 1)(2^{m-1} - 1)}{(2^{2m-1} - 1)} \quad .$$

(ii) Follows immediately because

$$\frac{2^{2m+1} - 2^{m+1} - 2^m + 1}{(2^{2m+1} - 1)} > \frac{2^{2m-1} - 2^m - 2^{m-1} + 1}{(2^{2m-1} - 1)}$$

is easily verified.

$$\begin{aligned} (iii) \quad \lim_{m \rightarrow \infty} a_m &= \lim_{m \rightarrow \infty} \frac{2^{2m-1} - 2^m - 2^{m-1} + 1}{2^{2m-1} - 1} \\ &= \lim_{m \rightarrow \infty} \frac{1 - \frac{2^m}{2^{2m-1}} - \frac{2^{m-1}}{2^{2m-1}} - \frac{1}{2^{2m-1}}}{1 - \frac{1}{2^{2m-1}}} \\ &= 1 \quad . \end{aligned}$$

Example 2.2.1. Let $m = 4$; then we have,

$$D_{3,9} = \begin{bmatrix} 1 & 1 & 1 \\ y & z & w \\ y^2 & z^2 & w^2 \\ \vdots & \vdots & \vdots \\ y^{14} & z^{14} & w^{14} \\ \hline \vdots & \vdots & \vdots \\ \hline y^{90} & z^{90} & w^{90} \\ \vdots & \vdots & \vdots \\ y^{104} & z^{104} & w^{104} \end{bmatrix} = \begin{bmatrix} 1000 & 100 & 10 \\ 0100 & 010 & 01 \\ 0010 & 001 & 11 \\ \vdots & \vdots & \vdots \\ 1001 & 100 & 11 \\ \hline \vdots & \vdots & \vdots \\ \hline 1000 & 101 & 10 \\ \vdots & \vdots & \vdots \\ 1001 & 101 & 11 \end{bmatrix}$$

where $y^4 + y + 1$ is the characteristic polynomial for the elements y^i , $z^3 + z + 1$ is the characteristic polynomial for the elements z^i , and $w^2 + w + 1$ is the characteristic polynomial for the elements w^i . Thus $y^4 = y + 1$ and so from Theorem 2.2.1 it follows that $D_{3,9}$ possesses property B_3 . From Theorem 2.2.2 we have that

$$a_4 = \frac{(2^4 - 1)(2^3 - 1)}{(2^7 - 1)} = \frac{105}{127} = .827 \quad .$$

Thus, $D_{3,9}$ is a parity check matrix for a binary group code with 105 message places, 9 redundancy places, and efficiency of .827, which corrects errors occurring in bursts of 3 or less.

Example 2.2.2. Let $m = 5$; then we have

$$D_{3,11} = \begin{bmatrix} 1 & 1 & 1 \\ y & z & w \\ \vdots & \vdots & \vdots \\ y^{30} & z^{30} & w^{30} \\ \hline \vdots & \vdots & \vdots \\ \hline y^{434} & z^{434} & w^{434} \\ \vdots & \vdots & \vdots \\ y^{464} & z^{464} & w^{464} \end{bmatrix} = \begin{bmatrix} 10000 & 1000 & 10 \\ 01000 & 0100 & 01 \\ \vdots & \vdots & \vdots \\ 01001 & 1000 & 10 \\ \hline \vdots & \vdots & \vdots \\ \hline 10000 & 1001 & 11 \\ \vdots & \vdots & \vdots \\ 01001 & 1001 & 11 \end{bmatrix}$$

where $y^5 + y^2 + 1$ is the characteristic polynomial for the elements y^i and $z^4 + z + 1$ is the characteristic polynomial for the elements z^i . Here m is odd, and so, since $z^4 = z + 1$, it follows from Theorem 2.2.1 that $D_{3,11}$ possesses property B_3 . From Theorem 2.2.2 we have that

$$a_5 = \frac{(2^5 - 1)(2^4 - 1)}{(2^9 - 1)} = \frac{465}{511} = .910$$

Thus, $D_{3,11}$ is a parity check matrix for a binary group code with 465 message places, 11 redundancy places, and an efficiency of .910, which corrects errors in bursts of 3 or less.

Example 2.2.3. Let $m = 10$; then if we take for the elements y^i the characteristic polynomial $y^{10} + y^3 + 1$, and $y' = y^5$, we have

$$D_{3,21} = \begin{bmatrix} 1 & 1 & 1 \\ y' & z & w \\ y'^2 & z^2 & w^2 \\ \vdots & \vdots & \vdots \\ y'^{522,752} & z^{522,752} & w^{522,752} \end{bmatrix}$$

where we take as the characteristic polynomial for z , $z^9 + z^8 + z^4 + z^3 + z^2 + z + 1$. Since m is even, and since $y'^{921} = y' + 1$, it follows from Theorem 2.2.1 that $D_{3,21}$ possesses property B_3 . From Theorem 2.2.2 we have

$$a_{10} = \frac{(2^{10} - 1)(2^9 - 1)}{(2^{19} - 1)} = \frac{522,753}{524,287} = .997$$

Thus, $D_{3,21}$ is a parity check matrix for the binary group code with 522,753 message places and 21 redundancy places, and an efficiency of .997, which corrects errors in bursts of 3 or less.

2.3. Binary Group Codes which Correct Errors in Bursts of Four or or Less for the Following Redundancies: $r_1 = 3k_1 + 1$,

$$r_2 = 4k_2 \text{ and } r_3 = 4k_3 + 3, \text{ where } k_1 \geq 3, k_2 \geq 3, \text{ and } k_3 \geq 2.$$

Reiger [14] has constructed parity check matrices for the following binary group codes which correct errors in bursts of 4 or less: (1) $r = 8$, $n = 18$; (2) $r = 9$, $n = 34$; (3) $r = 9$, $n = 38$; and (4) $r = 10$, $n = 64$. The methods developed in this section will show how we can obtain a binary group code which corrects errors in

bursts of 4 or less for which $r = 10$, $n = 73$, thus bettering Reiger's code for redundancy 10. His codes for $r = 8$ and $r = 9$ have as yet not been bettered.

Consider the matrix $D_4 = D_4(n \times r)$ where the elements of D_4 are elements of $GF(2)$. We can write D_4 as follows:

$$D_4 = \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{bmatrix},$$

where each α_i is a row vector of dimension $1 \times r$ with elements from $GF(2)$. By Theorem 1.2.1 a necessary and sufficient condition that the binary group code corresponding to D_4 correct all single bursts of errors of length 4 or less is that the following sets of vectors be distinct:

$$(2.7) \quad \epsilon_{i1}^{D_4}, \epsilon_{i2}^{D_4}, \epsilon_{i3}^{D_4}, \epsilon_{i4}^{D_4}, \epsilon_{i5}^{D_4}, \epsilon_{i6}^{D_4}, \epsilon_{i7}^{D_4}, \epsilon_{i8}^{D_4},$$

where $i = 1, \dots, n$, and where

$$\begin{array}{c} * \\ \downarrow \\ \epsilon_{i1} = (0, 0, \dots, 1, \dots, 0) \end{array},$$

$$\begin{array}{c} * \\ \downarrow \\ \epsilon_{i2} = (0, 0, \dots, 1, 1, \dots, 0) \end{array},$$

$$\begin{array}{c} * \\ \downarrow \\ \epsilon_{i3} = (0, 0, \dots, 1, 0, 1, \dots, 0) \end{array},$$

$$\begin{array}{c}
 * \\
 \downarrow \\
 \epsilon_{i4} = (0, 0, \dots, 1, 1, 1, \dots, 0) \quad , \\
 \\
 * \\
 \downarrow \\
 \epsilon_{i5} = (0, 0, \dots, 1, 0, 0, 1, \dots, 0) \quad , \\
 \\
 * \\
 \downarrow \\
 \epsilon_{i6} = (0, 0, \dots, 1, 1, 0, 1, \dots, 0) \quad , \\
 \\
 * \\
 \downarrow \\
 \epsilon_{i7} = (0, 0, \dots, 1, 0, 1, 1, \dots, 0) \quad , \\
 \\
 * \\
 \downarrow \\
 \epsilon_{i8} = (0, 0, \dots, 1, 1, 1, 1, \dots, 0) \quad .
 \end{array}$$

The star indicates the i -th position of ϵ_{ij} , $j = 1, 2, \dots, 8$. Performing the required multiplications in (2.7), we obtain the following sets of vectors:

$$(2.8) \quad \alpha_i \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.9) \quad \alpha_i + \alpha_{i+1} \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.10) \quad \alpha_i + \alpha_{i+2} \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.11) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.12) \quad \alpha_i + \alpha_{i+3} \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.13) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+3} \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.14) \quad \alpha_i + \alpha_{i+2} + \alpha_{i+3} \quad , \quad i = 1, \dots, n \quad ;$$

$$(2.15) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} + \alpha_{i+3} \quad , \quad i = 1, \dots, n \quad .$$

Thus, if the vectors in (2.8)-(2.15) are all distinct, D_4 is the parity check matrix for the binary group code which corrects all single error bursts of length 4 or less where the number of message places is n and the number of redundancy places is r . This leads us to the following definition.

Definition 2.3.1. We shall say that the matrix D_4 possesses the property B_4 if the vectors in (2.8)-(2.15) are all distinct.

Thus, property B_4 is a necessary and sufficient condition for D_4 to be an appropriate parity check matrix for a binary group code that corrects all error vectors which contain a single burst of length 4 or less.

We consider first the case where $r = 3k_1 + 1$, $k_1 \geq 3$. Suppose that y is a primitive element of $GF(2^{3k_1})$, and let

$$D_{4,3k_1+1} = D_{4,3k_1+1} \left[\left(\frac{2^{3k_1} - 1}{7} \right) \times (3k_1 + 1) \right], \quad \text{be the following matrix}$$

$$D_{4,3k_1+1} = \begin{bmatrix} 1 & 1 \\ y^7 & 1 \\ y^{14} & 1 \\ \vdots & \vdots \\ y^{2^{3k_1-8}} & 1 \end{bmatrix},$$

where y^{7i} is equivalent to the $3k_1$ -vector, with elements from $GF(2)$, which is the coefficient vector of the $(3k_1-1)$ -th degree polynomial

in y representing y^{7^i} . Thus α_i as given in (2.8) is $(y^{7^i}, 1)$, $i = 0,$

$1, \dots, \frac{3k_1-1}{7} - 1$. Since 7 divides $2^{\frac{3k_1}{7}} - 1$, we can choose the 7-th powers of y and not destroy the cyclic property of $D_{4, 3k_1+1}$.

The placing of a one in the last position of α_i divides the vectors (2.8)-(2.15) into two classes for codes with these parity check matrices - those vectors with a one in the last position and those vectors with a zero in the last position. Thus, in obtaining conditions to assure that $D_{4, 3k_1+1}$ possess property B_4 , we need only obtain conditions for assuring that each class of vectors - those with a one in the last position and those with a zero in the last position - is distinct. We can now state the following definition.

Definition 2.3.2. We say that

$$(2.16) \quad \alpha_i + a_{i+1} \alpha_{i+1} + \dots + a_{i+\ell-2} \alpha_{i+\ell-2} + \alpha_{i+\ell-1},$$

$a_{i+j} \in GF(2)$, $j = 1, 2, \dots, \ell - 2$, is an even burst vector if (1) there is a one in the last position of α_{i+j} for $j = 0, 1, \dots, \ell - 1$, and (2) there are an even number of terms in (2.16). We say that (2.16) is an odd burst vector if (1) there is a one in the last position of α_{i+j} for $j = 0, 1, \dots, \ell - 1$, and (2) there are an odd number of terms in (2.16).

Thus, for the case $\alpha_i = (y^{7^i}, 1)$, $i = 0, 1, \dots, \frac{3k_1-1}{7} - 1$, we can divide (2.8)-(2.15) into even and odd burst vectors. We can now state and prove necessary and sufficient conditions that $D_{4, 3k_1+1}$

possess property B_4 .

Theorem 2.3.1. Let us set $\alpha_i = (y^{7i}, 1)$, $i = 0, 1, \dots, \frac{3k_1}{7} - 1$.

Now let us divide (2.8)-(2.15) into the even burst vectors and odd burst vectors as follows:

<u>Odd</u>	<u>Even</u>	
α_i	$= (y^{7i}, 1)$	$\alpha_i + \alpha_{i+1} = (y^{7i+a_4}, 0)$,
$\alpha_i + \alpha_{i+1} + \alpha_{i+2}$	$= (y^{7i+a_1}, 1)$	$\alpha_i + \alpha_{i+2} = (y^{7i+2a_4}, 0)$,
$\alpha_i + \alpha_{i+1} + \alpha_{i+3}$	$= (y^{7i+a_2}, 1)$	$\alpha_i + \alpha_{i+3} = (y^{7i+a_1+a_4}, 0)$,
$\alpha_i + \alpha_{i+2} + \alpha_{i+3}$	$= (y^{7i+a_3}, 1)$	$\alpha_i + \alpha_{i+1} + \alpha_{i+2} + \alpha_{i+3} = (y^{7i+3a_4}, 0)$,

where

$$\begin{aligned}
 1 + y^7 + y^{14} &= y^{a_1} & , & & 1 + y^7 &= y^{a_4} & , \\
 1 + y^7 + y^{21} &= y^{a_2} & , & & 1 + y^{14} &= y^{2a_4} & , \\
 1 + y^{14} + y^{21} &= y^{a_3} & , & & 1 + y^{21} &= y^{a_1+a_4} & , \\
 & & & & 1 + y^7 + y^{14} + y^{21} &= y^{3a_4} & .
 \end{aligned}$$

Then necessary and sufficient conditions that $D_{4, 3k_1+1}$ possess property B_4 are:

- (1) $0, a_1, a_2,$ and a_3 are all distinct (mod 7);
- (2) $0, a_4, 2a_4$ and a_1 are all distinct (mod 7).

Proof. Condition (1) is necessary and sufficient to insure that the odd burst vectors are all distinct, and condition (2) is necessary and sufficient to insure that all the even burst vectors are

distinct. Thus (1) and (2) taken together are precisely conditions that $D_{4,3k_1+1}$ possess property B_4 .

We now calculate the efficiency of these codes.

Theorem 2.3.2. Let the efficiency of the code corresponding to $D_{4,3k_1+1}$ be given as b_{3k_1+1} . Then

$$(i) \quad b_{3k_1+1} = \frac{(2^{3k_1} - 1)}{7(2^{3k_1-2} - 1)}$$

(ii) $b_{3k_1+1} < b_{3(k_1-1)+1}$, i.e., b_{3k_1+1} is a strictly decreasing integer function of k_1 ;

$$(iii) \quad \lim_{k_1 \rightarrow \infty} b_{3k_1+1} = 4/7.$$

Proof. (i) By Definition 1.4.1, $b_{3k_1+1} = n/n_0$, where

$$n = \frac{2^{3k_1} - 1}{7}$$

and

$$n_0 = \left[\frac{2^{3k_1+1} - 1}{2^3} \right] = 2^{3k_1-2} - 1.$$

Thus, $b_{3k_1+1} = \frac{2^{3k_1} - 1}{7(2^{3k_1-2} - 1)}$. (ii) and (iii) are proved in a manner

completely analogous to the proof of (2) and (3) in Theorem 2.2.2.

We present the following example of this method.

Example 2.3.1. Let $k_1 = 3$; then $r = 10$, and $D_{4,10}$ is given as

$$D_{4,10} = \begin{bmatrix} 1 & 1 \\ y^7 & 1 \\ y^{14} & 1 \\ \vdots & \vdots \\ y^{504} & 1 \end{bmatrix},$$

where y is a primitive element of $GF(2^9)$ satisfying the characteristic polynomial $y^9 + y^8 + y^4 + y^3 + y^2 + y + 1 = 0$. With the characteristic polynomial as given above, we have:

<u>Odd</u>		<u>Even</u>
$1 + y^7 + y^{14} = y^{375}$,	$1 + y^7 = y^{29}$
$1 + y^7 + y^{21} = y^{379}$,	$1 + y^{14} = y^{58}$
$1 + y^{14} + y^{21} = y^{34}$,	$1 + y^{21} = y^{404}$
		$1 + y^7 + y^{14} + y^{21} = y^{27}$

Thus $a_1 = 475$, $a_2 = 379$, $a_3 = 34$ and $a_4 = 29$. Hence, 0, 375, 379 and 34 are all distinct (mod 7) and 0, 29, 58 and 375 are all distinct (mod 7). Thus, by Theorem 2.3.1 and Theorem 1.2.1, $D_{4,10}$ represents an appropriate parity check matrix for the binary group code which corrects all error vectors containing a single error burst of length 4 or less, where $n = 73$, $r = 10$. We note that Reiger [14] constructs a parity check matrix for the binary group code which corrects all error vectors containing a single error burst of length 4 or less, where $n = 64$, $r = 10$. Thus the code represented by $D_{4,10}$ represents an improvement over Reiger's code in that we obtain 9 extra message places at no extra redundancy cost.

The efficiency of the above code is

$$b_{10} = \frac{2^9 - 1}{7(2^7 - 1)} = \frac{73}{127} = .574 \quad .$$

We next consider the case where $r = 4k_2$, $k_2 \geq 3$. Let y be a primitive element of the Galois field $\text{GF}(2^{4k_2-4})$ and let z be a primitive element of the subfield $\text{GF}(2^4)$ of $\text{GF}(2^{4k_2-4})$. Again we should note that y^i is equivalent to the $(4k_2 - 4)$ -vector, with elements from $\text{GF}(2)$, which is the coefficient vector of the $(4k_2 - 5)$ -th degree polynomial in y corresponding to y^i . Similarly, z^i is equivalent to the 4-vector, with elements from $\text{GF}(2)$ which is the coefficient vector of the 3-rd degree polynomial in z corresponding to z^i . Now let

$$D_{4,4k_2} = D_{4,4k_2} \left[(2^{4k_2-4} - 1) \times 4k_2 \right] \quad \text{be the following matrix:}$$

$$D_{4,4k_2} =$$

$$\begin{bmatrix} 1 & 1 \\ y & z \\ \vdots & \vdots \\ y^{14} & z^{14} \\ \hline y^{15} & 1 \\ y^{16} & z \\ \vdots & \vdots \\ y^{29} & z^{14} \\ \hline \vdots & \vdots \\ \hline 2^{\frac{4k_2-4}{2}} y^{-16} & 1 \\ \vdots & \vdots \\ y^2 2^{\frac{4k_2-4}{2}} - 2 & z^{14} \end{bmatrix}$$

Thus α_i as given in (2.8) is (y^i, z^i) where $z^{15} = 1$, $i = 0, 1, \dots,$

$2^{\frac{4k_2-4}{2}} - 2$. For matrices of the form $D_{4,4k_2}$ there is no column of 1's

added, so that in considering necessary and sufficient conditions that

$D_{4,4k_2}$ have property B_4 , we cannot consider odd and even burst vectors.

We now state and prove necessary and sufficient conditions that

$D_{4,4k_2}$ have property B_4 .

Theorem 2.3.3. Let us set $\alpha_i = (y^i, z^i)$, $i = 0, 1, \dots, 2^{\frac{4k_2-4}{2}} - 2$.

Thus we can write (2.8)-(2.15) as follows:

$$(2.17) \quad \alpha_i = (y^i, z^i) ,$$

$$(2.18) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} = (y^{i+b_1}, z^{i+10}) ,$$

$$(2.19) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+3} = (y^{i+b_2}, z^{i+7}) ,$$

$$(2.20) \quad \alpha_i + \alpha_{i+2} + \alpha_{i+3} = (y^{i+b_3}, z^{i+13}) ,$$

$$(2.21) \quad \alpha_i + \alpha_{i+1} = (y^{i+b_4}, z^{i+4}) ,$$

$$(2.22) \quad \alpha_i + \alpha_{i+2} = (y^{i+2b_4}, z^{i+8}) ,$$

$$(2.23) \quad \alpha_i + \alpha_{i+3} = (y^{i+b_1+b_4}, z^{i+14}) ,$$

$$(2.24) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} + \alpha_{i+3} = (y^{i+3b_4}, z^{i+12}) ,$$

where $i = 0, 1, \dots, 2^{4k-4} - 2$, and where we set

$$1 + y + y^2 = y^{b_1} ,$$

$$1 + y + y^3 = y^{b_2} ,$$

$$1 + y^2 + y^3 = y^{b_3} ,$$

$$1 + y = y^{b_4} ;$$

and, using as a characteristic polynomial for the z 's $z^4 + z + 1$, we also have:

$$1 + z + z^2 = z^{10} ,$$

$$1 + z + z^3 = z^7 ,$$

$$1 + z^2 + z^3 = z^{13} ,$$

$$1 + z = z^4 .$$

Then, a necessary and sufficient condition that $D_{4,4k_2}$ have property B_4 is that $0, b_1-10, b_2-7, b_3-13, b_4-4, 2b_4-8, b_1+b_4-14$ and $3b_4-12$ are all distinct (mod 15).

Proof. (1) Suppose that $D_{4,4k_2}$ has property B_4 . Then the vectors (2.17)-(2.24) must be all distinct. In order for this to occur, we must have that $0, b_1-10, b_2-7, b_3-13, b_4-4, 2b_4-8, b_1+b_4-14$, and $3b_4-12$ are all distinct mod 15.

(2) Conversely, if these eight quantities are all distinct mod 15, then the vectors (2.17)-(2.24) must be all distinct, that is, $D_{4,4k_2}$ has property B_4 .

If, for a given primitive element y of $GF(2^{4k_2})$, the quantities $0, b_1-10, b_2-7, b_3-13, b_4-4, 2b_4-8, b_1+b_4-14, 3b_4-12$ are not all distinct mod 15, it is often possible to find a new primitive element $y' = y^\tau$, where τ and $2^{4k_2} - 1$ are relatively prime, such that the condition is satisfied for the primitive element y' . It has not been proved that such an element will exist for all k_2 , but we do show it does exist for $k_2 = 3$ in the example below.

Example 2.3.2. Suppose $k_2 = 3$. Let y be the primitive element of $GF(2^8)$ which satisfies the characteristic polynomial equation $y^8 + y^4 + y^3 + y^2 + 1 = 0$, and, as in Theorem 2.3.3, let z be a primitive element of $GF(2^4)$ having $z^4 + z + 1$ as a characteristic polynomial in the field $GF(2^4)$. We cannot use y directly because the condition of Theorem 2.3.3 will not be satisfied. Thus we let $y' = y^7$ be our transformation. Since 255 and 7 have no common divisor > 1 , y' is again a primitive element of $GF(2^8)$. Now let $D_{4,12} = D_{4,12}(255 \times 12)$ be the

the following matrix:

$$D_{4,12} = \begin{bmatrix} 1 & 1 \\ y' & z \\ \vdots & \vdots \\ y',14 & z',14 \\ \hline y',15 & 1 \\ y',16 & z \\ \vdots & \vdots \\ y',30 & z',14 \\ \hline \vdots & \vdots \\ \hline y',240 & 1 \\ y',241 & z \\ \vdots & \vdots \\ y',254 & z',14 \end{bmatrix}$$

We thus obtain the following equations:

$$1 + y' + y'^2 = y',204 \quad ,$$

$$1 + y' + y'^3 = y',215 \quad ,$$

$$1 + y'^2 + y'^3 = y',125 \quad ,$$

$$1 + y' = y',16 \quad .$$

Thus, $b_1 = 204$, $b_2 = 215$, $b_3 = 125$, and $b_4 = 16$. Hence,

$$(2.25) \quad b_1 - 10 = 194 - 14 \pmod{15} \quad ,$$

$$(2.26) \quad b_2 - 7 = 208 = 13 \pmod{15} \quad ,$$

$$(2.27) \quad b_3 - 13 = 112 = 7 \pmod{15} \quad ,$$

$$(2.28) \quad b_4 - 4 = 12 = 12 \pmod{15} \quad ,$$

$$(2.29) \quad 2b_4 - 8 = 24 = 9 \pmod{15} \quad ,$$

$$(2.30) \quad b_1 + b_4 - 14 = 206 = 11 \pmod{15} \quad ,$$

$$(2.31) \quad 3b_4 - 12 = 36 = 6 \pmod{15} \quad .$$

Thus, (2.25)-(2.31) show that $0, b_1 - 10, b_2 - 7, b_3 - 13, b_4 - 4, 2b_4 - 8, b_1 + b_4 - 14,$ and $3b_4 - 12$ are all distinct $\pmod{15}$, insuring that $D_{4,12}$ possesses property B_4 . Thus, by Theorem 1.2.1, $D_{4,12}$ is an appropriate parity check matrix for the binary group code which corrects all error vectors containing a single burst of length less than or equal to 4, where $n = 255$ and $r = 12$.

We now derive the efficiency of the codes represented by $D_{4,4k_2}$.

Theorem 2.3.4. Let the efficiency of the code corresponding to $D_{4,4k_2}$ be given as b_{4k_2} . Then

$$(i) \quad b_{4k_2} = \frac{2^{4k_2-4} - 1}{2^{4k_2-3} - 1} \quad ,$$

$$(ii) \quad b_{4(k_2+1)} > b_{4k_2} \quad ,$$

$$(iii) \quad \lim_{k_2 \rightarrow \infty} b_{4k_2} = 1/2 \quad .$$

Proof. (i) By Definition 1.4.1 $b_{4k_2} = n/n_0$, where $n = 2^{4k_2-4} - 1$

and

$$n_0 = \left[\frac{2^{4k_2} - 1}{2^3} \right] = 2^{4k_2-3} - 1.$$

Thus $b_{4k_2} = \frac{2^{4k_2-4}}{2^{4k_2-3} - 1}$. (ii) and (iii) follow immediately from (i).

For the code described in Example 2.3.2 we have $b_{12} = \frac{255}{511} = .499$.

To conclude this section we show how the method of "cycling" is used to construct parity check matrices for binary group codes possessing property B_4 with redundancies of the form $4k_3 + 3$, $k_3 \geq 2$. We shall first need the following lemma.

Lemma 2.3.1. Let m be an even integer ≥ 4 ; then $\frac{2^m - 1}{3}$ and $\frac{2^{m-2} - 1}{3}$ are relatively prime.

Proof. Any divisor of $\frac{2^m - 1}{3}$ and $\frac{2^{m-2} - 1}{3}$ must divide their difference. However, we have that $\frac{2^m - 1}{3} - \frac{2^{m-2} - 1}{3} = 2^{m-2}$, a pure power of 2, whereas $\frac{2^m - 1}{3}$ and $\frac{2^{m-2} - 1}{3}$ are both odd. Thus the only possible common divisor for these numbers is 1.

Let (y^{3^i}, z^{3^i}) , $i = 0, 1, \dots, \left(\frac{2^{2k_3+2}}{3} - 1\right)\left(\frac{2^{2k_3}}{3} - 1\right) - 1$, be a cycle; then, by Lemmas 2.2.1 and 2.3.1, the vectors (y^{3^i}, z^{3^i}) ,

$i = 0, 1, \dots, \left(\frac{2^{2k_3+2}}{3} - 1\right)\left(\frac{2^{2k_3}}{3} - 1\right) - 1$, form a cycle of length

$(\frac{2^{2k_3+2}}{3} - 1)(\frac{2^{2k_3} - 1}{3})$. Hence, defining the matrix $D_{4,4k_3+3} =$

$D_{4,4k_3+3} \left[\ell \times (4k_3 + 3) \right]$, where $\ell = \frac{(2^{2k_3+2} - 1)(2^{2k_3} - 1)}{9}$, as

$$D_{4,4k_3+3} = \begin{bmatrix} 1 & 1 & 1 \\ y^3 & z^3 & 1 \\ \vdots & \vdots & \vdots \\ y^{2^{2k_3+2} - 4} & z^{2^{2k_3+2} - 4} & 1 \\ \vdots & \vdots & \vdots \\ y^{3(\ell-1)} & z^{3(\ell-1)} & 1 \end{bmatrix}$$

all the row vectors in $D_{4,4k_3+3}$ are distinct. We can now state necessary and sufficient conditions that the matrix $D_{4,4k_3+3}$ possess property B_4 .

Theorem 2.3.5. We can set $\alpha_i = (y^{3i}, z^{3i}, 1)$, $i = 0, 1, \dots$,

$v_1 v_2 = 1$, where $v_1 = \frac{2^{2k_3+2} - 1}{3}$ and $v_2 = \frac{2^{2k_3} - 1}{3}$. Since as 1 occurs in the last place of α_i for all i , we can divide the vectors (2.8) - (2.15) into even and odd burst vectors as follows:

Odd

$$(2.32) \quad \alpha_i = (y^{3i}, z^{3i}, 1)$$

$$(2.33) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} = (y^{3i+c_1}, z^{3i+d_1}, 1)$$

$$(2.34) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+3} = (y^{3i+c_2}, z^{3i+d_2}, 1)$$

$$(2.35) \quad \alpha_i + \alpha_{i+2} + \alpha_{i+3} = (y^{3i+c_3}, z^{3i+d_3}, 1)$$

Even

$$(2.36) \quad \alpha_i + \alpha_{i+1} = (y^{3i+c_4}, z^{3i+d_4}, 0)$$

$$(2.37) \quad \alpha_i + \alpha_{i+2} = (y^{3i+2c_4}, z^{3i+2d_4}, 0)$$

$$(2.38) \quad \alpha_i + \alpha_{i+3} = (y^{3i+c_1+c_4}, z^{3i+d_1+d_4}, 0)$$

$$(2.39) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} + \alpha_{i+3} = (y^{3i+3c_4}, z^{3i+3d_4}, 0)$$

where $c_1, c_2, c_3, c_4, d_1, d_2, d_3$ and d_4 are defined as follows:

$$1 + y^3 + y^6 = y^{c_1},$$

$$1 + y^3 + y^9 = y^{c_2},$$

$$1 + y^6 + y^9 = y^{c_3},$$

$$1 + y^3 = y^{c_4},$$

$$1 + z^3 + z^6 = z^{d_1},$$

$$1 + z^3 + z^9 = z^{d_2},$$

$$1 + z^6 + z^9 = z^{d_3},$$

$$1 + z^3 = z^{d_4},$$

Then necessary and sufficient conditions that $D_{4,4k_3+3}$ possess property B_4 are:

(1) $(0,0)$, (c_1, d_1) , (c_2, d_2) , and (c_3, d_3) are distinct two-place vectors, where each c_i and d_i is reduced mod 3;

(2) (c_4, d_4) , $(2c_4, 2d_4)$, $(c_1 + c_4, d_1 + d_4)$, and $(3c_4, 3d_4)$ are distinct two-place vectors, where again each component of each vector is reduced mod 3.

Proof. Condition (1) is necessary and sufficient to insure that all the odd burst vectors are distinct, and condition (2) is necessary and sufficient to insure that all the even burst vectors are distinct. Thus (1) and (2) taken together are necessary and sufficient that $D_{4,4k_3+3}$ have property B_4 .

We now calculate the efficiency of these codes.

Theorem 2.3.6. Let the efficiency of the code corresponding to $D_{4,4k_3+3}$ be given as b_{4k_3+3} . Then

$$(i) \quad b_{4k_3+3} = \frac{(2^{\frac{2k_3+2}{3}} - 1)(2^{\frac{2k_3}{3}} - 1)}{9(2^{\frac{4k_3}{3}} - 1)},$$

$$(ii) \quad b_{4(k_3+1)+3} > b_{4k_3+3}$$

$$(iii) \quad \lim_{k_3 \rightarrow \infty} b_{4k_3+3} = 4/9$$

Proof. (i) follows immediately from Definition 1.4.1 since

$$n = \frac{(2^{2k_3+2} - 1)(2^{2k_3} - 1)}{9}, \quad n_0 = \left[\frac{2^{4k_3+3} - 1}{2^3} \right] = 2^{4k_3} - 1.$$

(ii) and (iii) follow easily from (i).

Example 2.3.3. Let $k_3 = 2$; then $D_{4,11}$ is given as follows:

$$D_{4,11} = \begin{bmatrix} 1 & 1 & 1 \\ y^3 & z^3 & 1 \\ \vdots & \vdots & \vdots \\ y^{312} & z^{312} & 1 \end{bmatrix},$$

where y is a primitive element of $GF(2^6)$ and has as its characteristic polynomial $y^6 + y + 1$, and z is a primitive element of $GF(2^4)$ and its characteristic polynomial is $z^4 + z + 1$. We thus have the following:

$$\begin{aligned} 1 + y^3 + y^6 &= y^{13}, \\ 1 + y^3 + y^9 &= y^{24}, \\ 1 + y^6 + y^9 &= y^{49}, \\ 1 + y^3 &= y^{32}, \\ 1 + z^3 + z^6 &= z^8, \\ 1 + z^3 + z^9 &= z^4, \\ 1 + z^6 + z^9 &= z^{10}, \\ 1 + z^3 &= z^{14}. \end{aligned}$$

Thus,

$$\begin{aligned} c_1 &= 13, & c_2 &= 24, & c_3 &= 49, & c_4 &= 32; \\ d_1 &= 8, & d_2 &= 4, & d_3 &= 10, & d_4 &= 14. \end{aligned}$$

Condition (1) of the theorem is satisfied because $(0,0)$, $(13,8)$, $(24,4)$, $(49,10)$ are distinct vectors, where each element of each vector is reduced mod 3. Condition (2) is also satisfied since $(32,14)$; $(1,13)$; $(45,7)$; $(33,12)$ are distinct vectors where each element of each vector is reduced mod 3. Thus, $D_{4,11}$ possesses property B_4 and hence is an appropriate parity check matrix for the binary group code with $n = 105$, $r = 11$, which corrects all error vectors containing a single burst of length 4 or less. The efficiency of this code is:

$$b_{11} = \frac{105}{255} = .412 \quad .$$

Example 2.3.4. Let $k_3 = 3$; then $D_{4,15}$ is given as follows:

$$D_{4,15} = \begin{bmatrix} 1 & 1 & 1 \\ y^{13} & z^3 & 1 \\ \vdots & \vdots & \vdots \\ y^{5352} & z^{5352} & 1 \end{bmatrix}$$

where y is a primitive element of $GF(2^8)$ and has as its characteristic polynomial $y^8 + y^4 + y^3 + y^2 + 1$, and z is a primitive element of $GF(2^6)$ and has as its characteristic polynomial $z^6 + z + 1$. In order to satisfy Theorem 2.3.5 it was necessary to transform y and z into new primitive elements $y' = y^{13}$, and $z' = z^5$. We thus obtain the following:

$$\begin{aligned}
1 + y^3 + y^6 &= y^{217} , \\
1 + y^3 + y^9 &= y^{27} , \\
1 + y^6 + y^9 &= y^{101} , \\
1 + y^3 &= y^{67} , \\
1 + z^3 + z^6 &= z^{35} , \\
1 + z^3 + z^9 &= z^2 , \\
1 + z^6 + z^9 &= z^{48} , \\
1 + z^3 &= z^{55} .
\end{aligned}$$

Thus,

$$\begin{aligned}
c_1 &= 217, & c_2 &= 27, & c_3 &= 101, & c_4 &= 67 ; \\
d_1 &= 35, & d_2 &= 2, & d_3 &= 48, & d_4 &= 55 .
\end{aligned}$$

Condition (1) of the theorem is satisfied because $(0,0)$; $(217,35)$; $(27,2)$; $(101,48)$ are distinct vectors, where each element of each vector is reduced mod 3. Similarly it is easily shown that condition (2) of the theorem is also satisfied. Thus $D_{4,15}$ possesses property B_4 and hence is an appropriate parity check matrix for the binary group code, with $n = 1785$ and $r = 15$, which corrects all error vectors containing a single burst of length 4 or less. The efficiency of this code is:

$$b_{15} = \frac{1785}{4095} = .436 .$$

CHAPTER III

P-NARY LINEAR CODES WHICH CORRECT ERRORS IN BURSTS OF LENGTH d OR LESS, FOR $p = 3, 5$, AND $d = 2$, AND FOR $p = 3$, $d = 3$.

3.1. Golay Codes.

Golay [10] describes the following method for the construction of single-error-correcting p-nary codes. Let $E_{1,m+1}^p = E_{1,m+1}^p \begin{bmatrix} (p^m - 1) \\ \times (m + 1) \end{bmatrix}$ be the following matrix:

$$E_{1,m+1}^p = \begin{bmatrix} 1 & 1 \\ y & 1 \\ y^2 & 1 \\ \vdots & \vdots \\ y^{p^m - 2} & 1 \end{bmatrix},$$

where y is a primitive element of $GF(p^m)$, $p > 2$, and the last column is filled by a column of ones. Again we should note that y^i is equivalent to the m -vector, with elements from $GF(p)$, which is the coefficient vector of the $(m-1)$ -th degree polynomial in y representing y^i . Now, by Theorem 1.2.1, a necessary and sufficient condition that $E_{1,m+1}^p$ be an appropriate parity check matrix for the p-nary linear code, with $n = p^m - 1$, $r = m + 1$, which corrects all single errors, is that the vectors

$$\begin{aligned} \delta_i &= [y^i, 1] \\ 2\delta_i &= [2y^i, 2] \\ &\vdots \\ (p-1)\delta_i &= [(p-1)y^i, p-1] \end{aligned} .$$

be all distinct for $i = 0, 1, \dots, p^m - 2$. These vectors are all distinct because

(i) each set

$$k\delta_i = [ky^i, k] \quad ,$$

$1 \leq k \leq p-1$, $i = 0, 1, \dots, p^m - 2$, contains p distinct vectors since ky^i represents all the distinct non-zero elements of $GF(p^m)$ as i goes from 0 to $p^m - 2$,

$$(ii) \quad k\delta_{i_1} = [ky^{i_1}, k] \neq j\delta_{i_2} = [jy^{i_2}, j]$$

for any $i_1 \neq i_2$ and $k \neq j$, since these vectors differ in the last place.

The efficiency of these codes is derived from Definition 1.4.1 as follows. $n = p^m - 1$, and

$$n_0 = \left[\frac{p^{m+1} - 1}{p - 1} \right] = \frac{p^{m+1} - 1}{p - 1} \quad ;$$

therefore, letting c_{m+1}^p represent the efficiency of these codes, we have

$$(3.1) \quad c_{m+1}^p = \frac{(p^m - 1)(p - 1)}{(p^{m+1} - 1)} \quad .$$

Clearly, (3.1) is a strictly increasing function of m and:

$$\lim_{m \rightarrow \infty} c_{m+1}^p = \frac{p - 1}{p} \quad .$$

Example 3.1.1. For an example of a Golay code, let $p = 3$ and $m = 2$; then $E_{1,3}^3$ is given by

$$E_{1,3}^3 = \begin{bmatrix} 1 & 1 \\ y & 1 \\ y^2 & 1 \\ y^3 & 1 \\ y^4 & 1 \\ y^5 & 1 \\ y^6 & 1 \\ y^7 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 2 & 1 \\ 2 & 0 & 1 \\ 0 & 2 & 1 \\ 2 & 2 & 1 \\ 2 & 1 & 1 \end{bmatrix},$$

using the characteristic polynomial $y^2 - y - 1$ for y . Hence, $E_{1,3}^3$ represents an appropriate parity check matrix for the ternary linear code, $n = 8$, $r = 3$, which corrects all error vectors containing a single error. By (3.1) we have:

$$c_3^3 = \frac{(3^2 - 1)(3 - 1)}{3^3 - 1} = \frac{16}{26} = .615.$$

3.2. Ternary Linear Codes Which Correct Consecutive Errors in Bursts of Two or Less

Thus far there is no general method for constructing p -nary linear codes which correct all error vectors containing a single burst of length two or less. However, in this section and in Section 3.3 we shall derive methods for obtaining such codes when $p = 3$ and $p = 5$.

Let $E_{2,r}^3 = E_{2,r}^3(n \times r)$ be the following matrix:

$$E_{2,r}^3 = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix},$$

where α_i , $i = 0, 1, \dots, n-1$, is a $1 \times r$ row vector with elements from $GF(3)$. Then a necessary and sufficient condition that $E_{2,r}^3$ be an appropriate parity check matrix for the ternary linear code which corrects all error vectors containing a single burst of length two or less is that

$$(3.2) \quad \alpha_i \quad ,$$

$$(3.3) \quad 2\alpha_i \quad ,$$

$$(3.4) \quad \alpha_i + \alpha_{i+1} \quad ,$$

$$(3.5) \quad 2\alpha_i + 2\alpha_{i+1} \quad ,$$

$$(3.6) \quad \alpha_i + 2\alpha_{i+1} \quad ,$$

$$(3.7) \quad 2\alpha_i + \alpha_{i+1} \quad ,$$

all be distinct vectors for $i = 0, 1, \dots, n-1$. This follows from Theorem 1.2.1 after we perform the required matrix multiplications of the form $\epsilon_{ij} E_{2,r}^3$ for $i = 0, 1, \dots, n-1$ and $j = 1, 2, \dots, 6$, where

$$\begin{array}{c} * \\ \downarrow \\ \epsilon_{i1} = (0, 0, \dots, 0, 1, 0, \dots, 0) \quad , \end{array}$$

$$\begin{array}{c} * \\ \downarrow \\ \epsilon_{i2} = (0, 0, \dots, 0, 2, 0, \dots, 0) \quad , \end{array}$$

$$\begin{array}{c}
 * \\
 \downarrow \\
 \epsilon_{i3} = (0, 0, \dots, 0, 1, 1, 0, \dots, 0) \quad , \\
 * \\
 \downarrow \\
 \epsilon_{i4} = (0, 0, \dots, 0, 2, 2, 0, \dots, 0) \quad , \\
 * \\
 \downarrow \\
 \epsilon_{i5} = (0, 0, \dots, 0, 1, 2, 0, \dots, 0) \quad , \\
 * \\
 \downarrow \\
 \epsilon_{i6} = (0, 0, \dots, 0, 2, 1, 0, \dots, 0) \quad ,
 \end{array}$$

in which the star denotes the i -th position of ϵ_{ij} . This leads us now to the following definition.

Definition 3.2.1. We say that the matrix $E_{2,r}^3$ possesses property T_2 if the vectors in (3.2)-(3.7) are all distinct.

For codes with even redundancy, Elspas [8] describes the following method for constructing ternary linear codes which correct all single errors and all double adjacent errors. Let $E_{2,m+1}^3$ be the matrix $E_{2,m+1}^3 = E_{2,m+1}^3 \left[\left(\frac{3^m - 1}{2} \right) \times (m+1) \right]$ given by

$$E_{2,m+1}^3 = \begin{bmatrix} 1 & 1 \\ y^2 & 1 \\ y^4 & 1 \\ \vdots & \vdots \\ y^{3m-3} & 1 \end{bmatrix}$$

where y is a primitive element of $GF(3^m)$, $m \geq 3$ is odd, and the last

column is a column of ones. Again we should note that y^i is equivalent to the m -vector, with elements from $\text{GF}(3)$, which is the coefficient vector of the $(m-1)$ -th degree polynomial in y representing y^i . We are now in a position to state and prove the following theorem.

Theorem 3.2.1. A necessary and sufficient condition that $E_{2,m+1}^3$, m odd, possess property T_2 is that there exist some primitive element y of $\text{GF}(3^m)$ such that $1 + y^2 = y^{2k}$, i.e., $1 + y^2$ is an even power of y .

Proof. For the matrix $E_{2,m+1}^3$, the vector sets (3.2)-(3.7) become:

$$(3.2') \quad \alpha_i = \left[y^{2i}, 1 \right],$$

$$(3.3') \quad 2\alpha_i = \left[2y^{2i}, 2 \right] = \left[y^{2i + \frac{3^m - 1}{2}}, 2 \right],$$

$$(3.4') \quad \alpha_i + \alpha_{i+1} = \left[y^{2i}(1 + y^2), 2 \right],$$

$$(3.5') \quad 2\alpha_i + 2\alpha_{i+1} = \left[2y^{2i}(1 + y^2), 1 \right] = \left[y^{2i + \frac{3^m - 1}{2}}(1 + y^2), 1 \right],$$

$$(3.6') \quad \alpha_i + 2\alpha_{i+1} = \left[y^{2i}(1 + 2y^2), 0 \right],$$

$$(3.7') \quad 2\alpha_i + \alpha_{i+1} = \left[y^{2i}(2 + y^2), 0 \right] = \left[y^{2i + \frac{3^m - 1}{2}}(1 + 2y^2), 0 \right].$$

First of all, the elements of each vector set are distinct because

$$\text{each of } y^{2i}, y^{2i + \frac{3^m - 1}{2}}, y^{2i}(1 + y^2), y^{2i + \frac{3^m - 1}{2}}(1 + y^2),$$

$y^{2i}(1 + 2y^2)$ and $y^{2i + \frac{3^m - 1}{2}}(1 + 2y^2)$, $i = 0, 1, \dots, \frac{3^m - 1}{2} - 1$, represents $\frac{3^m - 1}{2}$ distinct non-zero elements from $\text{GF}(3^m)$. By comparing the last place of each vector set we see that no element from the set (3.2') could be equal to any element of the sets (3.3'), (3.4'), (3.6'), or (3.7'). Similar comparisons hold for the sets (3.3') and (3.4') compared with the sets (3.5'), (3.6'), and (3.7'), and also for the set (3.5') compared with the sets (3.6') and (3.7'). Further, since m is odd, $(3^m - 1)/2$ is odd so that no element of (3.6') could be equal to any element of (3.7'). If, say, the j -th element of the set (3.3') were equal to the k -th element of the set (3.4'), then

$$y^{2j + \frac{3^m - 1}{2}} = y^{2k}(1 + y^2) \quad ;$$

this can occur if and only if $1 + y^2$ is an odd power of y . Similarly, the j -th element of the set (3.2') will be equal to the k -th element of the set (3.5') if and only if $1 + y^2$ is an odd power of y . Hence, a necessary and sufficient condition that $E_{2,m+1}^3$ possess property T_2 is that $1 + y^2$ be an even power of y .

We now derive the efficiency of these codes. By Definition 1.4.1 we have

$$n = \frac{3^m - 1}{2} \quad , \quad n_o = \left[\frac{3^{m+1} - 1}{6} \right] \quad ,$$

since $r = m + 1$, and $s = 3$. Thus,

$$n_o = \frac{3^m - 1}{2} \quad ,$$

and $n/n_0 = 1$. These codes thus have maximum efficiency.

Example 3.2.1. Let $m = 3$ and let y be the primitive element of $GF(3^3)$ with characteristic polynomial $y^3 - y - 2$. Since $1 + y^2 = y^{21}$ for this characteristic polynomial, we need make a transformation $y' = y^\tau$ such that 26 and τ are relatively prime and $1 + y'^2 = y'^{2k}$ so that the condition of Theorem 3.2.1 is satisfied. Such a transformation is $y' = y^5$, for which $1 + y'^2 = y'^{22}$. We can thus write $E_{2,4}^3$ as follows:

$$E_{2,4}^3 = \begin{array}{|l} 1 \\ y'^2 \\ y'^4 \\ y'^6 \\ y'^8 \\ y'^{10} \\ y'^{12} \\ y'^{14} \\ y'^{16} \\ y'^{18} \\ y'^{20} \\ y'^{22} \\ y'^{24} \end{array} \begin{array}{|l} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{array} = \begin{array}{|l} 100 \\ 011 \\ 112 \\ 021 \\ 020 \\ 122 \\ 202 \\ 121 \\ 001 \\ 201 \\ 220 \\ 111 \\ 120 \end{array} \begin{array}{|l} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{array}$$

Thus, by Theorem 3.2.1 and Theorem 1.2.1, $E_{2,4}^3$ is an appropriate parity check matrix for the ternary linear code, $n = 13$, $r = 4$, which corrects all error vectors containing bursts of length two or less.

Example 3.2.2. Let $m = 5$ and let y be the primitive element of $\text{GF}(3^5)$ with characteristic polynomial $y^5 - y - 2$. We then have $1 + y^2 = y^{46}$, so that we can write $E_{2,6}^3$ as

$$E_{2,6}^3 = \begin{bmatrix} 1 & 1 \\ y^2 & 1 \\ y^4 & 1 \\ y^6 & 1 \\ \vdots & \vdots \\ y^{240} & 1 \end{bmatrix} = \begin{bmatrix} 10000 & 1 \\ 00100 & 1 \\ 00001 & 1 \\ 01200 & 1 \\ \vdots & \vdots \\ 10022 & 1 \end{bmatrix} .$$

Hence, by Theorem 3.2.1, $E_{2,6}^3$ possesses property T_2 , and thus, by Theorem 1.2.1, $E_{2,6}^3$ is a parity check matrix for the ternary linear code, $n = 121$, $r = 6$, which corrects all single and double adjacent errors.

We now use the method of cycles to obtain ternary linear codes which correct consecutive errors in bursts of two or less when the redundancy is odd and of the form $4m_1 + 1$.

Lemma 3.2.1. Suppose that m is odd, $m \geq 3$; then the integers $3^m - 1$ and $(3^{m-2} - 1)/2$ are relatively prime.

Proof. Let d be the greatest common divisor of $3^m - 1$ and $(3^{m-2} - 1)/2$. Then d cannot be even since $(3^{m-2} - 1)/2$ is odd, and also d cannot be a multiple of 3. It follows that d must divide the difference $(3^m - 1) - (3^{m-2} - 1) = 2 \cdot 3^{m-2}$ and this implies that $d = 1$.

Thus, by Lemmas 3.2.1 and 2.2.1, (y^i, z^{2i}) , $i = 0, 1, \dots, (l-1)$,

form a cycle of length $\frac{(3^m - 1)(3^{m-2} - 1)}{2}$, where y is a primitive element of $\text{GF}(3^m)$, z is a primitive element of $\text{GF}(3^{m-2})$, m is odd and greater than or equal to 5, and $\ell = \frac{(3^m - 1)(3^{m-2} - 1)}{2}$. Let us now set $m = 2m_1 + 1$, $m_1 \geq 2$. We can now state and prove the following theorem.

Theorem 3.2.2. Let $E_{2,4m_1+1}^3 = E_{2,4m_1+1}^3 \left[\frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} \times (4m_1 + 1) \right]$ be the following matrix:

$$E_{2,4m_1+1}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y & z^2 & 1 \\ y^2 & z^4 & 1 \\ \vdots & \vdots & \vdots \\ y^{\ell-1} & z^{2\ell-2} & 1 \end{bmatrix} .$$

Then a necessary and sufficient condition that $E_{2,4m_1+1}^3$ possess property T_2 is that $1 + z^2$ be an even power of z .

Proof. Let us define δ_i as

$$\delta_i = (y^i, z^{2i}, 1)$$

for $i = 0, 1, \dots, \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} - 1$. First of all, the elements of the vector set $\{\delta_i\}$ are all distinct, since (y^i, z^{2i}) ,

$i = 0, 1, \dots, \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} - 1$, form a cycle of length

$\frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2}$. Now consider the vectors of the form

$$\begin{aligned}\delta_i + \delta_{i+1} &= \left[y^i(1+y), z^{2i}(1+z^2), 2 \right] \\ &= \left[y^{i+\rho}, z^{2i+\phi}, 2 \right],\end{aligned}$$

say, for $i = 0, 1, \dots, \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} - 1$. The elements of this vector set are all distinct, for if

$$\delta_{i_1} + \delta_{i_1+1} = \delta_{i_2} + \delta_{i_2+1}, \quad i_1 \neq i_2,$$

$0 \leq i_1, i_2 \leq \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} - 1$, then the equations

$$\begin{aligned}y^{i_1+\rho} &= y^{i_2+\rho}, \\ z^{2i_1+\phi} &= z^{2i_2+\phi},\end{aligned}$$

hold simultaneously, or, equivalently, the equations

$$\begin{aligned}y^{i_1} &= y^{i_2}, \\ z^{2i_1} &= z^{2i_2},\end{aligned}$$

hold simultaneously for $i_1 \neq i_2$, $0 \leq i_1, i_2 \leq \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} - 1$,

which contradicts that (y^i, z^{2i}) , $i = 0, 1, \dots, \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2} - 1$,

form a cycle of length $\frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2}$. Similarly, elements of the vector sets

$$\begin{aligned} & \{ 2\delta_i \} \quad , \\ & \{ 2\delta_i + 2\delta_{i+1} \} \quad , \\ & \{ \delta_i + 2\delta_{i+1} \} \quad , \\ & \{ 2\delta_i + \delta_{i+1} \} \quad , \end{aligned}$$

are all distinct. As in the proof of Theorem 3.2.1, elements of the sets $\{ \delta_i \}$ and $\{ 2\delta_i + 2\delta_{i+1} \}$ can not be equal to elements of the other sets since the elements of these sets have a 1 in their last positions whereas the elements of the other sets have either a 0 or 2 in their last positions. Similarly, elements of the sets $\{ 2\delta_i \}$ and $\{ \delta_i + \delta_{i+1} \}$ cannot be equal to elements of the other sets, and elements of the sets $\{ \delta_i + 2\delta_{i+1} \}$ and $\{ 2\delta_i + \delta_{i+1} \}$ cannot be equal to elements of the other sets. The remaining possibilities for equalities between vectors are then

$$\begin{aligned} \delta_i + \delta_{i+1} &= 2\delta_j && \text{for some } i, j \quad , \\ 2\delta_k + 2\delta_{k+1} &= \delta_l && \text{for some } k, l \quad , \\ \delta_m + 2\delta_{m+1} &= 2\delta_n + \delta_{n+1} && \text{for some } m, n \quad . \end{aligned}$$

Now we can rule out the last equation, for if

$$\delta_m + 2\delta_{m+1} = 2\delta_n + \delta_{n+1} \quad ,$$

then

$$\begin{aligned} y^m(1 + 2y) &= y^n(2 + y) \quad , \\ z^{2m}(1 + 2z^2) &= z^{2n}(2 + z^2) \quad , \end{aligned}$$

would hold simultaneously, but then, since $(3^{2m-1} - 1)/2$ is odd and

since we can rewrite $z^{2m}(1 + 2z^2)$ as $z^{2m+(3^{2m_1-1} - 1)/2}(2 + z^2)$, we obtain an impossibility, for we obtain the equation

$$z^{2m+(3^{2m_1-1} - 1)/2} = z^{2n} .$$

Hence, the elements of the set $\{ \delta_i + 2\delta_{i+1} \}$ are distinct from the elements of the set $\{ 2\delta_i + \delta_{i+1} \}$. Now suppose that for some i, j we have

$$\delta_i + \delta_{i+1} = 2\delta_j .$$

This implies that the equations

$$y^i(1 + y) = y^{j + \frac{3^{2m_1+1} - 1}{2}} ,$$

$$z^{2i}(1 + z^2) = z^{2j + \frac{3^{2m_1-1} - 1}{2}} ,$$

hold simultaneously. Now, since $\frac{3^{2m_1-1} - 1}{2}$ is odd,

$$z^{2i}(1 + z^2) = z^{2j + \frac{3^{2m_1-1} - 1}{2}}$$

can hold if and only if $1 + z^2$ is an odd power of z . Similarly, we can show that

$$2\delta_k + 2\delta_{k+1} = \delta_l$$

holds if and only if $1 + z^2$ is an odd power of z . Thus we have that a necessary and sufficient condition that $E_{2, 4m_1+1}^3$ possess property T_2

is that $1 + z^2$ be an even power of z .

Hence, by Theorems 3.2.2 and 1.2.1, $E_{2,4m_1+1}^3$, $m_1 \geq 2$, represents an appropriate parity check matrix for the ternary linear code,

$n = \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2}$ and $r = 4m_1 + 1$, which corrects consecutive errors occurring in bursts of two or less, provided $1 + z^2$ is an even power of z .

We now derive the efficiency of these codes.

Theorem 3.2.3. Let c_{4m_1+1} be the efficiency of the code represented by $E_{2,4m_1+1}^3$. Then

$$(i) \quad c_{4m_1+1} = \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{(3^{4m_1} - 1)},$$

$$(ii) \quad c_{4(m_1+1)+1} > c_{4m_1+1},$$

$$(iii) \quad \lim_{m_1 \rightarrow \infty} c_{4m_1+1} = 1.$$

Proof. (i) By Definition 1.4.1, $c_{4m_1+1} = n/n_0$, where

$$n = \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{2},$$

$$n_0 = \left[\frac{3^{4m_1+1} - 1}{6} \right] = \frac{3^{4m_1} - 1}{2}.$$

Therefore,

$$c_{4m_1+1} = \frac{(3^{2m_1+1} - 1)(3^{2m_1-1} - 1)}{(3^{4m_1} - 1)}.$$

(ii) and (iii) follow immediately from (i).

Now suppose the redundancy is odd and of the form $4m_2 - 1$, $m_2 \geq 3$.

Lemma 3.2.2. The numbers $3^{2m_2+1} - 1$ and $(3^{2m_2-3} - 1)/2$ are relatively prime.

Proof. First of all we note that 5 cannot divide $3^{2k+1} - 1$, for $3^{2k+1} - 1 = 3 \cdot 9^k - 1 = 2 \pmod{10}$ if k is even, and $3^{2k+1} - 1 = 3 \cdot 9^k - 1 = 6 \pmod{10}$ if k is odd. To show that the g.c.d. of $3^{2m_2+1} - 1$ and $(3^{2m_2-3} - 1)/2$ is one, it suffices to show the g.c.d. of $3^{2m_2+1} - 1$ and $3^{2m_2-3} - 1$ is 2. If d is the g.c.d. of $3^{2m_2+1} - 1$ and $3^{2m_2-3} - 1$, then d must divide the difference $(3^{2m_2+1} - 1) - (3^{2m_2-3} - 1) = 3^{2m_2-3} \cdot 80$. But neither 3 nor 5 divides either $(3^{2m_2+1} - 1)$ or $(3^{2m_2-3} - 1)$; hence the only possible g.c.d. of these numbers is 2^k , where $k \leq 4$. However, since $(3^{2m_2+1} - 1)/2$ and $(3^{2m_2-3} - 1)/2$ are both odd, this implies that $d = 2$.

Thus, by Lemma 3.2.1 and Lemma 2.2.1, (y^i, z^{2i}) , $i = 0, 1, \dots$,

$$\frac{(3^{2m_2+1} - 1)(3^{2m_2-3} - 1)}{2} - 1 \text{ form a cycle of length } \frac{(3^{2m_2+1} - 1)(3^{2m_2-3} - 1)}{2},$$

where y is a primitive element of $\text{GF}(3^{2m_2+1})$ and z is a primitive element of $\text{GF}(3^{2m_2-3})$.

Theorem 3.2.4. Let $E_{2,4m_2-1}^3 = E_{2,4m_2-1}^3 \left[\frac{(3^{2m_2+1} - 1)(3^{2m_2-3} - 1)}{2} \right]$
 $\times (4m_2 - 1) \right]$, be the following matrix:

$$E_{2,4m_2-1}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y & z^2 & 1 \\ y^2 & z^4 & 1 \\ \vdots & \vdots & \vdots \\ y^{\ell-1} & z^{2^{\ell-2}} & 1 \end{bmatrix}$$

where $\ell = \frac{(3^{2m_2+1} - 1)(3^{2m_2-3} - 1)}{2}$. Then a necessary and sufficient condition that $E_{2,4m_2-1}^3$ possess property T_2 is that $1 + z^2$ be an even power of z , where y is a primitive element of $GF(3^{2m_2+1})$ and z is a primitive element of $GF(3^{2m_2-3})$.

The proof is analogous to that of Theorem 3.2.2 and hence is omitted. We now derive the efficiency of these codes.

Theorem 3.2.5. Let c_{4m_2-1} be the efficiency of the code represented by $E_{2,4m_2-1}^3$. Then

$$(i) \quad c_{4m_2-1} = \frac{(3^{2m_2+1} - 1)(3^{2m_2-3} - 1)}{3^{2m_2-2} - 1},$$

$$(ii) \quad c_{4(m_2+1)-1} > c_{4m_2-1},$$

$$(iii) \quad \lim_{m_2 \rightarrow \infty} c_{4m_2-1} = 1.$$

The proof is analogous to that of Theorem 3.2.3 and so is omitted.

Example 3.2.3. Let $m_1 = 2$; then y is a primitive element of $GF(3^5)$ and z is a primitive element of $GF(3^3)$, where we take the

characteristic polynomial for z as $z^3 - z - 2$. Since $1 + z^2 = z^{21}$ for this characteristic polynomial, we need to make a transformation $z' = z^\tau$ such that 26 and τ are relatively prime and $1 + z'^2 = z'^{2k}$, so that the condition of Theorem 3.2.2 is satisfied. Such a transformation is $z' = z^5$, for $1 + z'^2 = z'^{22}$. We can thus write $E_{2,9}^3$ as

$$E_{2,9}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y & z'^2 & 1 \\ y^2 & z'^4 & 1 \\ \vdots & \vdots & \vdots \\ y^{3145} & z'^{6290} & 1 \end{bmatrix} = \begin{bmatrix} 10000 & 100 & 1 \\ 01000 & 011 & 1 \\ 00100 & 112 & 1 \\ \vdots & \vdots & \vdots \\ 10002 & 120 & 1 \end{bmatrix},$$

where we note that (1) $y^{242} = z'^{26} = 1$, (2) the characteristic polynomial for y is $y^5 - y - 2$, and (3) there is equivalence between non-zero elements of the Galois field $GF(3^m)$ and non-zero m -vectors over $GF(3)$. Thus, $E_{2,9}^3$ is an appropriate parity check matrix for the ternary linear code, $n = 3146$, $r = 9$, which corrects all single and double adjacent errors, since by Theorem 3.2.2 $E_{2,9}^3$ possesses property T_3 and hence, by Theorem 1.2.1, is the required parity check matrix.

$$c_9 = \frac{(3^5 - 1)(3^3 - 1)}{(3^8 - 1)} = \frac{6292}{6560} = .959.$$

Thus, the code represented by $E_{2,9}^3$ has an efficiency of .959.

Example 3.2.4. Let $m_2 = 3$; then y is a primitive element of $GF(3^7)$ and z is a primitive element of $GF(3^3)$, where again the characteristic polynomial for z is $z^3 - z - 2$. Hence, we again make the transformation $z' = z^5$ so that $1 + z'^2 = z'^{22}$, in order to satisfy the

condition of Theorem 3.2.4. We thus write $E_{2,11}^3$ as

$$E_{2,11}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y & z^2 & 1 \\ y^2 & z^4 & 1 \\ \vdots & \vdots & \vdots \\ y^{28,417} & z^{56,834} & 1 \end{bmatrix} .$$

We note that we can reduce the elements y and z by the relationship $y^{2186} = z^{26} = 1$. Thus, by Theorem 3.2.4, $E_{2,11}^3$ possesses property T_2 , and hence, by Theorem 1.2.1, $E_{2,11}^3$ represents an appropriate parity check matrix for the ternary linear code, $n = 28,418$, $r = 11$, which corrects all single errors and double adjacent errors.

$$c_{11} = \frac{(3^7 - 1)(3^3 - 1)}{(3^{10} - 1)} = \frac{56,836}{59,048} = .964 .$$

Thus, the code represented by $E_{2,11}^3$ has an efficiency of .964.

Example 3.2.5. To conclude this section we shall give an example of a ternary linear code for redundancy 7. It should be noted that 9 is the minimum possible odd redundancy for either Theorem 3.2.2 or Theorem 3.2.4 to apply. Hence, the code constructed for $r = 7$ is constructed differently from the other codes in this section. Let y be a primitive element of $GF(3^4)$ and z be a primitive element of $GF(3^3)$. Let us consider the vectors (y^{5i}, z^{2i}) , $i = 0, 1, \dots, 207$. These vectors form a cycle of length 208, because $(3^4 - 1)/5 = 16$ and $(3^3 - 1)/2 = 13$ are relatively prime. Now let $E_{2,7}^3$ be the following matrix:

$$E_{2,7}^3 = \begin{bmatrix} 1 & 1 \\ y^5 & z^2 \\ \vdots & \vdots \\ y^{1035} & z^{414} \end{bmatrix} = \begin{bmatrix} 1000 & 100 \\ 2020 & 001 \\ \vdots & \vdots \\ 1121 & 102 \end{bmatrix},$$

where we note (1) the characteristic polynomials for y and z are, respectively, $y^4 + 2y^3 + 2y^2 + y + 1$ and $z^3 + z + 2$, (2) $y^{80} = z^{26} = 1$, and (3) there is equivalence between the non-zero elements of $\text{GF}(3^m)$ and the non-zero m -vectors over $\text{GF}(3)$. To show that $E_{2,7}^3$ possesses property T_2 we need show that all the vectors in the vector sets

$$(3.8) \quad \alpha_i = [y^{5i}, z^{2i}] ,$$

$$(3.9) \quad \alpha_i + \alpha_{i+1} = [y^{5i}(1 + y^5), z^{2i}(1 + z^2)] ,$$

$$(3.10) \quad 2\alpha_i = [2y^{5i}, 2z^{2i}] ,$$

$$(3.11) \quad 2\alpha_i + 2\alpha_{i+1} = [2y^{5i}(1 + y^5), 2z^{2i}(1 + z^2)] ,$$

$$(3.12) \quad \alpha_i + 2\alpha_{i+1} = [y^{5i}(1 + 2y^5), z^{2i}(1 + 2z^2)] ,$$

$$(3.13) \quad 2\alpha_i + \alpha_{i+1} = [y^{5i}(2 + y^5), z^{2i}(2 + z^2)] ,$$

$i = 0, 1, \dots, 207$, are distinct. We note the following relations:

$$1 + y^5 = y^{42} ,$$

$$1 + z^2 = z^{21} ,$$

$$1 + 2y^5 = y^{58} ,$$

$$1 + 2z^2 = z^{25} .$$

Thus, (3.8)-(3.13) become:

$$(3.8') \quad \alpha_i = (y^{5i}, z^{2i}) ,$$

$$(3.9') \quad \alpha_i + \alpha_{i+1} = (y^{5i+42}, z^{2i+21}) ,$$

$$(3.10') \quad 2\alpha_i = (y^{5i+40}, z^{2i+13}) ,$$

$$(3.11') \quad 2\alpha_i + 2\alpha_{i+1} = (y^{5i+2}, z^{2i+8}) ,$$

$$(3.12') \quad \alpha_i + 2\alpha_{i+1} = (y^{5i+58}, z^{2i+25}) ,$$

$$(3.13') \quad 2\alpha_i + \alpha_{i+1} = (y^{5i+18}, z^{2i+12}) ,$$

$i = 0, 1, \dots, 207$, and it follows that all these vectors are distinct since $(0,0)$, $(42,21)$, $(40,13)$, $(2,8)$, $(58,25)$, and $(18,12)$ represent distinct two-place vectors where the first component of each vector is reduced mod 5 and the second component of each vector is reduced mod 2. That these vectors are distinct within each set follows from the fact that (y^{5i}, z^{2i}) , $i = 0, 1, \dots, 207$, form a cycle of length 208. Thus, $E_{2,7}^3$ is an appropriate parity check matrix for the ternary linear code, $n = 208$, $r = 7$, which corrects all single and double adjacent errors.

$$c_7 = \frac{208}{364} = .571 .$$

Hence, the efficiency of the code represented by $E_{2,7}^3$ is .571 - considerably less than for those codes with greater odd redundancy.

3.3. Quintary Linear Codes Which Correct Consecutive Errors in Bursts of Two or Less for Even Redundancy and Odd Redundancy of the Form $4m + 1$.

We first need some results concerning the primitive elements of $GF(5^m)$. If y is a primitive element of $GF(5^m)$, then $y^{(5^m-1)/2} = 4$. Depending upon the characteristic polynomial chosen for y , we will have either: (1) $y^{(5^m-1)/4} = 3$ and $y^{3(5^m-1)/4} = 2$, or (2) $y^{(5^m-1)/4} = 2$ and $y^{3(5^m-1)/4} = 3$. For example, if $m = 2$, and the characteristic polynomial for the primitive element y is $y^2 - 2y - 2$, then $y^{(5^2-1)/4} = y^6 = 3$ and $y^{3(5^2-1)/4} = y^{18} = 2$; and if $m = 5$, and the characteristic polynomial for the primitive element y is $y^5 - y - 2$ then $y^{(5^5-1)/4} = y^{781} = 2$ and $y^{3(5^5-1)/4} = y^{2343} = 3$.

Let $E_{2,r}^5 = E_{2,r}^5$ ($n \times r$) be the following matrix:

$$E_{2,r}^5 = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix},$$

where α_i is a $1 \times r$ row vector with elements in $GF(5)$, $i = 0, 1, \dots, n-1$. Then a necessary and sufficient condition that $E_{2,r}^5$ be an appropriate parity check matrix for the quintary linear code which corrects consecutive errors in bursts of two or less is that

- (3.14) α_i ,
- (3.15) $3\alpha_i + 3\alpha_{i+1}$,
- (3.16) $2\alpha_i + 4\alpha_{i+1}$,
- (3.17) $4\alpha_i + 2\alpha_{i+1}$,
- (3.18) $2\alpha_i$,
- (3.19) $\alpha_i + \alpha_{i+1}$,
- (3.20) $4\alpha_i + 3\alpha_{i+1}$,
- (3.21) $3\alpha_i + 4\alpha_{i+1}$,
- (3.22) $3\alpha_i$,
- (3.23) $4\alpha_i + 4\alpha_{i+1}$,
- (3.24) $\alpha_i + 2\alpha_{i+1}$,
- (3.25) $2\alpha_i + \alpha_{i+1}$,
- (3.26) $4\alpha_i$,
- (3.27) $2\alpha_i + 2\alpha_{i+1}$,
- (3.28) $3\alpha_i + \alpha_{i+1}$,
- (3.29) $\alpha_i + 3\alpha_{i+1}$,
- (3.30) $2\alpha_i + 3\alpha_{i+1}$,
- (3.31) $4\alpha_i + \alpha_{i+1}$,
- (3.32) $\alpha_i + 4\alpha_{i+1}$,
- (3.33) $3\alpha_i + 2\alpha_{i+1}$,

$i = 0, 1, \dots, n-1$, all be distinct vectors. Thus, we are led to the following definition.

Definition 3.3.1. We say the matrix $E_{2,r}^5$ possesses property Q_2 if the vectors (3.14)-(3.33) are all distinct for $i = 0, 1, \dots, n-1$.

Let us first assume that the redundancy r is even and can be written as $r = 2m_1$, where $m_1 \geq 3$, is odd. We now state and prove the

following lemma.

Lemma 3.3.1. $(5^{m_1} - 1)/4$ and $(5^{m_1-1} - 1)/2$ are relatively prime.

Proof. Since $(5^{m_1} - 1)/4$ is odd, it suffices to show that the g.c.d. of $5^{m_1} - 1$ and $5^{m_1-1} - 1$ is 4. This follows immediately, for, if d is the g.c.d. of $5^{m_1} - 1$ and $5^{m_1-1} - 1$, d must divide $(5^{m_1} - 1) - (5^{m_1-1} - 1) = 5^{m_1-1} \cdot 4$, whence $d = 4$.

Thus, by Lemmas 3.3.1 and 2.2.1, (y^{4i}, z^{2i}) , $i = 0, 1, \dots, \frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{8} - 1$, form a cycle of length $\frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{8}$,

and hence we can formulate the following theorem.

Theorem 3.3.1. Let $E_{2,2m_1}^5$, where $m_1 \geq 3$, is odd, be the following matrix:

$$E_{2,2m_1}^5 = \begin{bmatrix} 1 & 1 & 1 \\ y^4 & z^2 & 1 \\ y^8 & z^4 & 1 \\ \vdots & \vdots & \vdots \\ y^{4\ell-4} & z^{2\ell-2} & 1 \end{bmatrix}$$

where $\ell = \frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{8}$, y is a primitive element of $\text{GF}(5^{m_1})$

and z is a primitive element of $\text{GF}(5^{m_1-1})$. Consider now the following equations:

$$3 + 3y^4 = y^{a_1} \quad ,$$

$$3 + 3z^2 = z^{b_1} \quad ,$$

$$2 + 4y^4 = y^{a_2} \quad ,$$

$$2 + 4z^2 = z^{b_2} \quad ,$$

$$4 + 2y^4 = y^{a_3} \quad ,$$

$$4 + 2z^2 = z^{b_3} \quad .$$

Then, a necessary and sufficient condition that $E_{2,2m_1}^5$ possess property Q_2 is that (a_0, b_0) , (a_1, b_1) , (a_2, b_2) , and (a_3, b_3) be distinct vectors where a_i is reduced mod 4 and b_i is reduced mod 2, $i = 0, 1, 2, 3$, and where $a_0 = b_0 = 0$.

Before proving Theorem 3.3.1 we should note that y^i is equivalent to the m_1 -vector, with elements from $GF(5)$, which is the coefficient vector of the (m_1-1) -th degree polynomial in y representing y^i , and that z^i is equivalent to the (m_1-1) -vector with elements from $GF(5)$, which is the coefficient vector of the (m_1-2) -th degree polynomial in z representing z^i .

Proof of Theorem 3.3.1. For the matrix $E_{2,2m_1}^5$, (3.14)-(3.33) become:

$$(3.14') \quad \alpha_i = (y^{4i}, z^{2i}, 1) \quad ,$$

$$(3.15') \quad 3\alpha_i + 3\alpha_{i+1} = (y^{4i+a_1}, z^{2i+b_1}, 1) \quad ,$$

$$(3.16') \quad 2\alpha_i + 4\alpha_{i+1} = (y^{4i+a_2}, z^{2i+b_2}, 1) \quad ,$$

$$\begin{aligned}
(3.17') \quad 4\alpha_i + 2\alpha_{i+1} &= (y^{4i+a_3}, z^{2i+b_3}, 1) , \\
(3.18') \quad 2\alpha_i &= (y^{4i+\eta_1}, z^{2i+\xi_1}, 2) , \\
(3.19') \quad \alpha_i + \alpha_{i+1} &= (y^{4i+a_1+\eta_1}, z^{2i+b_1+\xi_1}, 2) , \\
(3.20') \quad 4\alpha_i + 3\alpha_{i+1} &= (y^{4i+a_2+\eta_1}, z^{2i+b_2+\xi_1}, 2) , \\
(3.21') \quad 3\alpha_i + 4\alpha_{i+1} &= (y^{4i+a_3+\eta_1}, z^{2i+b_3+\xi_1}, 2) , \\
(3.22') \quad 3\alpha_i &= (y^{4i+\eta_2}, z^{2i+\xi_2}, 3) , \\
(3.23') \quad 4\alpha_i + 4\alpha_{i+1} &= (y^{4i+a_1+\eta_2}, z^{2i+b_1+\xi_2}, 3) , \\
(3.24') \quad \alpha_i + 2\alpha_{i+1} &= (y^{4i+a_2+\eta_2}, z^{2i+b_2+\xi_2}, 3) , \\
(3.25') \quad 2\alpha_i + \alpha_{i+1} &= (y^{4i+a_3+\eta_2}, z^{2i+b_3+\xi_2}, 3) , \\
(3.26') \quad 4\alpha_i &= (y^{4i+\eta_3}, z^{2i+\xi_3}, 4) , \\
(3.27') \quad 2\alpha_i + 2\alpha_{i+1} &= (y^{4i+a_1+\eta_3}, z^{2i+b_1+\xi_3}, 4) , \\
(3.28') \quad 3\alpha_i + \alpha_{i+1} &= (y^{4i+a_2+\eta_3}, z^{2i+b_2+\xi_3}, 4) , \\
(3.29') \quad \alpha_i + 3\alpha_{i+1} &= (y^{4i+a_3+\eta_3}, z^{2i+b_3+\xi_3}, 4) , \\
(3.30') \quad 2\alpha_i + 3\alpha_{i+1} &= (y^{4i+c}, z^{2i+d}, 0) , \\
(3.31') \quad 4\alpha_i + \alpha_{i+1} &= (y^{4i+c+\eta_1}, z^{2i+d+\xi_1}, 0) , \\
(3.32') \quad \alpha_i + 4\alpha_{i+1} &= (y^{4i+c+\eta_2}, z^{2i+d+\xi_2}, 0) , \\
(3.33') \quad 3\alpha_i + 2\alpha_{i+1} &= (y^{4i+c+\eta_3}, z^{2i+d+\xi_3}, 0) ,
\end{aligned}$$

$i = 0, 1, \dots, \ell - 1$. Here $\eta_3 = 1/2(5^{m_1} - 1)$, $\xi_3 = 1/2(5^{m_1-1} - 1)$, and we may assume without loss of generality that $\eta_1 = 3/4(5^{m_1} - 1)$, $\xi_1 = 3/4(5^{m_1-1} - 1)$, $\eta_2 = 1/4(5^{m_1} - 1)$, and $\xi_2 = 1/4(5^{m_1-1} - 1)$.

First of all, each vector set contains $\ell = \frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{8}$ distinct vectors since (y^{4i}, z^{2i}) , $i = 0, \dots, \ell - 1$, form a cycle of length $\frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{8}$. Clearly, a necessary and sufficient condition that the sets (3.14')-(3.17') be distinct is that (a_0, b_0) , (a_1, b_1) , (a_2, b_2) , and (a_3, b_3) be distinct, where a_i is reduced mod 4 and b_i is reduced mod 2, $i = 0, 1, 2, 3$. Moreover, if (a_i, b_i) , $i = 0, 1, 2, 3$, are distinct for a_i reduced mod 4 and b_i reduced mod 2, then $(a_i + \eta_j, b_i + \xi_j)$, $j = 1, 2, 3$, must be distinct for fixed j , and conversely. Thus, a necessary and sufficient condition that the vectors in (3.14') - (3.29') be all distinct is that (a_0, b_0) , (a_1, b_1) , (a_2, b_2) and (a_3, b_3) be distinct, where a_i is reduced mod 4 and b_i is reduced mod 2. Finally, since m_1 is odd, $0, \eta_1, \eta_2$, and η_3 are all distinct mod 4, so that (3.30') - (3.33') are distinct vectors. This completes the proof of the theorem.

We now derive the efficiency of these codes.

Theorem 3.3.2. Let d_{2m_1} be the efficiency of the code represented by $E_{2,2m_1}^5$; then

$$(i) \quad d_{2m_1} = \frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{2(5^{m_1-1} - 1)},$$

$$(ii) \quad d_{2m_1+2} > d_{2m_1},$$

$$(iii) \quad \lim_{m_1 \rightarrow \infty} d_{2m_1} = 1/2.$$

Proof. By Definition 1.4.1, $d_{2m_1} = n/n_0$, where $n =$

$$\frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{8}, \quad n_0 = \left[\frac{5^{2m_1} - 1}{20} \right] = \frac{5^{2m_1-1} - 1}{4}. \quad \text{Hence,}$$

$$d_{2m_1} = \frac{(5^{m_1} - 1)(5^{m_1-1} - 1)}{2(5^{m_1-1} - 1)}. \quad (ii) \text{ and } (iii) \text{ follow immediately}$$

from (i).

Now suppose that $r = 2m_2$ and $m_2 \geq 4$ is even. Then by exactly the same argument as in Lemma 3.3.1 it follows that $(5^{m_2-1} - 1)/4$ and $(5^{m_2} - 1)/2$ are relatively prime. Thus, (y^{2i}, z^{4i}) form a cycle of length $\frac{(5^{m_2} - 1)(5^{m_2-1} - 1)}{8}$ for $i = 0, 1, \dots, \frac{(5^{m_2} - 1)(5^{m_2-1} - 1)}{8} - 1$, where y is a primitive element of $GF(5^{m_2})$ and z is a primitive element of $GF(5^{m_2-1})$. We now formulate the following theorem.

Theorem 3.3.3. Let $E_{2,2m_2}^5$, where $m_2 \geq 4$ is even, be the following matrix:

$$E_{2,2m_2}^5 = \begin{bmatrix} 1 & 1 & 1 \\ y^2 & z^4 & 1 \\ y^4 & z^8 & 1 \\ \vdots & \vdots & \vdots \\ y^{2\ell-2} & z^{4\ell-4} & 1 \end{bmatrix}$$

where $\ell = \frac{(5^{m_2} - 1)(5^{m_2-1} - 1)}{8}$. Consider now the following equations:

$$3 + 3y^2 = y^{a'_1} \quad ,$$

$$3 + 3z^4 = z^{b'_1} \quad ,$$

$$2 + 4y^2 = y^{a'_2} \quad ,$$

$$2 + 4z^4 = z^{b'_2} \quad ,$$

$$4 + 2y^2 = y^{a'_3} \quad ,$$

$$4 + 2z^4 = z^{b'_3} \quad .$$

Then, a necessary and sufficient condition that $E_{2,2m_2}^5$ possess property Q_2 is that (a'_0, b'_0) , (a'_1, b'_1) , (a'_2, b'_2) , and (a'_3, b'_3) be distinct vectors, where a'_i is reduced mod 2 and b'_i is reduced mod 4, $i = 0, 1, 2, 3$, and where $a'_0 = b'_0 = 0$.

The proof of Theorem 3.3.3 is exactly the same as that for Theorem 3.3.1 with the roles of y and z reversed, and so is omitted. Also, the efficiencies of these codes are exactly the same as for the codes represented in Theorem 3.3.1. Thus we have:

Theorem 3.3.4. Let d_{2m_2} be the efficiency of the code represented by $E_{2,2m_2}^5$; then

$$(i) \quad d_{2m_2} = \frac{(5^{m_2} - 1)(5^{m_2-1} - 1)}{2(5^{2m_2-1} - 1)} \quad ,$$

$$(ii) \quad d_{2m_2+2} > d_{2m_2} \quad ,$$

$$(iii) \quad \lim_{m_2 \rightarrow \infty} d_{2m_2} = 1/2 \quad .$$

Now let us suppose r is odd and let $r = 2m_3 + 1$, $m_3 \geq 4$ and even. We now state and prove the following lemma.

Lemma 3.3.2. $(5^{m_3+1} - 1)/4$ and $(5^{m_3-1} - 1)/2$ are relatively prime.

Proof. Since $(5^{m_3+1} - 1)/4$ is odd, it suffices to show that the g.c.d. of $5^{m_3+1} - 1$ and $5^{m_3-1} - 1$ is 4. If d is the g.c.d. of $5^{m_3+1} - 1$ and $5^{m_3-1} - 1$, then d must divide their difference

$$(5^{m_3+1} - 1) - 5^{m_3-1}(5^2 - 1) = 5^{m_3-1} \cdot 2^3 \cdot 3.$$

However, 3 divides neither $5^{m_3+1} - 1$ nor $5^{m_3-1} - 1$, since $m_3 + 1$ and $m_3 - 1$ are both odd. Clearly, 5 divides neither $5^{m_3+1} - 1$ nor $5^{m_3-1} - 1$, and the largest power of 2 which divides both $5^{m_3+1} - 1$ and $5^{m_3-1} - 1$ is $2^2 = 4$. Thus $d = 4$.

Hence, from Lemmas 3.3.2 and 2.2.1 it follows that (y^{4i}, z^{2i}) ,

$i = 0, \dots, \frac{(5^{m_3+1} - 1)(5^{m_3-1} - 1)}{8} - 1$ form a cycle of length

$\frac{(5^{m_3+1} - 1)(5^{m_3-1} - 1)}{8}$, where y is a primitive element of $GF(5^{m_3+1})$

and z is a primitive element of $GF(5^{m_3-1})$. We now formulate the following theorem.

Theorem 3.3.5. Let $E_{2, 2m_3+1}^5$, where $m_3 \geq 4$ is even, be the

following matrix:

$$E_{2,2m_3+1}^5 = \begin{bmatrix} 1 & 1 & 1 \\ y^4 & z^2 & 1 \\ y^8 & z^4 & 1 \\ \vdots & \vdots & \vdots \\ y^{4\ell-4} & z^{2\ell-2} & 1 \end{bmatrix},$$

where y is a primitive element of $GF(5^{\frac{m_3+1}{3}})$, z is a primitive element of $GF(5^{\frac{m_3-1}{3}})$, and $\ell = \frac{(5^{\frac{m_3+1}{3}} - 1)(5^{\frac{m_3-1}{3}} - 1)}{8}$. Consider the following equations:

$$3 + 3y^4 = y^{c_1},$$

$$3 + 3z^2 = z^{d_1},$$

$$2 + 4y^4 = y^{c_2},$$

$$2 + 4z^2 = z^{d_2},$$

$$4 + 2y^4 = y^{c_3},$$

$$4 + 2z^2 = z^{d_3}.$$

Then, a necessary and sufficient condition that $E_{2,2m_3+1}^5$ possess property Q_2 is that (c_0, d_0) , (c_1, d_1) , (c_2, d_2) , and (c_3, d_3) be distinct vectors, where c_i is reduced mod 4 and d_i is reduced mod 2, $i = 0, 1, 2, 3$, and $c_0 = d_0 = 0$. Again, the proof of Theorem 3.3.5 is completely analogous to that of Theorem 3.3.1, and so is omitted.

The efficiencies of these codes are obtained in a manner analogous to that by which the efficiencies were derived in Theorem 3.3.2; thus we obtain the following theorem.

Theorem 3.3.6. Let d_{2m_3+1} be the efficiency of the code represented by $E_{2,2m_3+1}^5$; then

$$(i) \quad d_{2m_3+1} = \frac{(5^{m_3+1} - 1)(5^{m_3-1} - 1)}{2(5^{2m_3} - 1)} \quad ,$$

$$(ii) \quad d_{2(m_3+1)+1} > d_{2m_3+1} \quad ,$$

$$(iii) \quad \lim_{m_3 \rightarrow \infty} d_{2m_3+1} = 1/2 \quad .$$

Example 3.3.1. Let $m_1 = 3$, and suppose that y is a primitive element of $GF(5^3)$ with characteristic polynomial $y^3 - 2y - 3$, and that z is a primitive element of $GF(5^2)$ with characteristic polynomial $z^2 - 2z - 2$. Now let $y' = y^7$ be a transformation of y to the new primitive element y' . Then we have

$$E_{2,6}^5 = \begin{bmatrix} 1 & 1 & 1 \\ y'^4 & z & 1 \\ \vdots & \vdots & \vdots \\ y',1484 & z^{742} & 1 \end{bmatrix} = \begin{bmatrix} 100 & 10 & 1 \\ 411 & 22 & 1 \\ \vdots & \vdots & \vdots \\ 322 & 12 & 1 \end{bmatrix} .$$

We thus have

$$\begin{aligned} 3 + 3y'^4 &= y',37 \quad , \\ 2 + 4y'^4 &= y',114 \quad , \\ 4 + 2y'^4 &= y' \quad , \end{aligned}$$

$$\begin{aligned} 3 + 3z^2 &= z^3 & , \\ 2 + 4z^2 &= z^7 & , \\ 4 + 2z^2 &= z^{16} & , \end{aligned}$$

so that we have $a_0 = b_0 = 0$; $a_1 = 1$, $a_2 = 2$, $a_3 = 1 \pmod{4}$; $b_1 = 1$, $b_2 = 1$, $b_3 = 0 \pmod{2}$. Thus, $(0,0)$, $(1,1)$, $(2,1)$, and $(1,0)$ are all distinct, and hence, by Theorem 3.3.1, $E_{2,6}^5$ possesses property Q_2 . That is, by Theorem 1.2.1, $E_{2,6}^5$ represents an appropriate parity check matrix for the quintary linear code, $n = 372$, $r = 6$, which corrects all single errors and all double adjacent errors. By Theorem 3.3.2 we have

$$d_6 = 372/781 = .478 \quad .$$

Hence, the efficiency of the code represented by $E_{2,6}^5$ is .478.

Example 3.3.2. Let $m_2 = 4$, and suppose that y is a primitive element of $GF(5^4)$ with characteristic polynomial $y^4 - y^3 - y - 2$, and that z is a primitive element of $GF(5^3)$ with characteristic polynomial $z^3 - 2z - 3$. Let $y' = y^7$ be a transformation of y to the new primitive element y' , and let $z' = z^7$ be the transformation of z to the new primitive element z' . Then we have

$$E_{2,8}^5 = \begin{bmatrix} 1 & 1 & 1 \\ y'^2 & z'^4 & 1 \\ \vdots & \vdots & \vdots \\ y',19,342 & z',38,684 & 1 \end{bmatrix} ,$$

and

$$\begin{aligned}
3 + 3y'^2 &= y',595 & , \\
2 + 4y'^2 &= y',475 & , \\
4 + 2y'^2 &= y',576 & , \\
3 + 3z'^4 &= z',37 & , \\
2 + 4z'^4 &= z',114 & , \\
4 + 2z'^4 &= z' & ;
\end{aligned}$$

Hence we have $a'_0 = b'_0 = 0$; $a'_1 = 1$, $a'_2 = 1$, $a'_3 = 0 \pmod{2}$; $b'_1 = 1$, $b'_2 = 2$, $b'_3 = 1 \pmod{4}$. Thus, $(0,0)$, $(1,1)$, $(1,2)$, and $(0,1)$ are all distinct, so that by Theorem 3.3.3, $E_{2,8}^5$ possesses property Q_2 . By Theorem 1.2.1 this give us that $E_{2,8}^5$ is an appropriate parity check matrix for the quintary linear code, $n = 9,672$, $r = 8$, which corrects all single errors and double adjacent errors. By Theorem 3.3.4 we have

$$d_8 = \frac{9,672}{19,531} = .495 \quad .$$

Hence, the efficiency of the code represented by $E_{2,8}^5$ is .495.

Example 3.3.3. Let $m_3 = 4$, and suppose that y is a primitive element of $GF(5^5)$ with characteristic polynomial $y^5 - y - 2$, and that z is a primitive element of $GF(5^3)$ with characteristic polynomial $z^3 - 2z - 3$. Let $y' = y^7$ be a transformation of y to the new primitive element y' and let $z' = z^3$ be a transformation of z to the new primitive element z' . Then we have

$$E_{2,9}^5 = \begin{bmatrix} 1 & 1 & 1 \\ y'^4 & z'^2 & 1 \\ \vdots & \vdots & \vdots \\ y',193,684 & z',96,842 & 1 \end{bmatrix}$$

and

$$\begin{aligned}
 3 + 3y' &= y', 2594 & , \\
 2 + 4y' &= y', 2750 & , \\
 4 + 2y' &= y', 928 & , \\
 3 + 3z' &= z', 36 & , \\
 2 + 4z' &= z', 13 & , \\
 4 + 2z' &= z', 89 & .
 \end{aligned}$$

Thus we have $c_0 = d_0 = 0$; $c_1 = 2$, $c_2 = 2$, $c_3 = 0 \pmod{4}$; $d_1 = 0$, $d_2 = 1$, and $d_3 = 1 \pmod{2}$. Hence, $(0,0)$, $(2,0)$, $(2,1)$, and $(0,1)$ are distinct two-place vectors, and so, by Theorem 3.3.5, $E_{2,9}^5$ possesses property Q_2 . That is, $E_{2,9}^5$ is an appropriate parity check matrix for the qunitary linear code, $n = 48,422$, $r = 9$, which corrects all single errors and double adjacent errors. By Theorem 3.3.6 we have

$$d_9 = \frac{48,422}{97,656} = .496 \quad .$$

Hence, the efficiency of the code represented by $E_{2,9}^5$ is .496.

3.4. Ternary Linear Codes Which Correct Errors in Bursts of Three or Less for Even Redundancy.

To conclude this chapter we discuss the problem of constructing parity check matrices for ternary linear codes, with even redundancy, which correct all single error bursts of length three or less.

Let $E_{3,r}^3$ be the following $n \times r$ matrix:

$$E_{3,4}^3 = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{n-1} \end{bmatrix}$$

where α_i , $i = 0, 1, \dots, n-1$, is a $1 \times r$ row vector with elements in $GF(3)$. Then a necessary and sufficient condition that $E_{3,r}^3$ be an appropriate parity check matrix for the ternary linear code, with n as its number of message places and r its redundancy, which corrects all error vectors containing a single burst of less than or equal to three in length is that the vectors

$$(3.34) \quad \alpha_i \quad ,$$

$$(3.35) \quad 2\alpha_i + 2\alpha_{i+1} \quad ,$$

$$(3.36) \quad 2\alpha_i + 2\alpha_{i+2} \quad ,$$

$$(3.37) \quad \alpha_i + \alpha_{i+1} + 2\alpha_{i+2} \quad ,$$

$$(3.38) \quad \alpha_i + 2\alpha_{i+1} + \alpha_{i+2} \quad ,$$

$$(3.39) \quad 2\alpha_i + \alpha_{i+1} + \alpha_{i+2} \quad ,$$

$$(3.40) \quad 2\alpha_i \quad ,$$

$$(3.41) \quad \alpha_i + \alpha_{i+1} \quad ,$$

$$(3.42) \quad \alpha_i + \alpha_{i+2} \quad ,$$

$$(3.43) \quad 2\alpha_i + 2\alpha_{i+1} + \alpha_{i+2} \quad ,$$

$$(3.44) \quad 2\alpha_i + \alpha_{i+1} + 2\alpha_{i+2} \quad ,$$

$$(3.45) \quad \alpha_i + 2\alpha_{i+1} + 2\alpha_{i+2} \quad ,$$

$$(3.46) \quad \alpha_i + 2\alpha_{i+1} \quad ,$$

$$(3.47) \quad \alpha_i + 2\alpha_{i+2} \quad ,$$

$$(3.48) \quad 2\alpha_i + \alpha_{i+1} \quad ,$$

$$(3.49) \quad 2\alpha_i + \alpha_{i+2} \quad ,$$

$$(3.50) \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} \quad ,$$

$$(3.51) \quad 2\alpha_i + 2\alpha_{i+1} + 2\alpha_{i+2} \quad ,$$

$i = 0, 1, \dots, n-1$, be all distinct. This follows from Theorem

1.2.1. We are thus led to the following definition.

Definition 3.4.1. We say the matrix $E_{3,r}^3$ possesses property T_3 if the vectors (3.34) - (3.51) are all distinct.

Lemma 3.4.1. Let k be an integer ≥ 1 ; then $(3^{2k+1} - 1)/2$ and $(3^4 - 1)/5 = 16$ are relatively prime.

Proof. $(3^{2k+1} - 1)/2$ is an odd number whereas $16 = 2^4$.

Thus, by Lemmas 2.2.1 and 3.4.1, (y^{2i}, z^{5i}) , for $i = 0, 1, \dots, 8(3^{2k+1} - 1) - 1$, form a cycle of length $8(3^{2k+1} - 1)$. Now let $E_{3,2k+6}^3$ be the following matrix:

$$E_{3,2k+6}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y^2 & z^5 & 1 \\ y^4 & z^{10} & 1 \\ \vdots & \vdots & \vdots \\ y^{2\ell-2} & z^{5\ell-5} & 1 \end{bmatrix} ,$$

where y is a primitive element of $GF(3^{2k+1})$, z is a primitive element of $GF(3^4)$, and the last column is filled by a one in each position, $\ell = 8(3^{2k+1} - 1)$. We then have the following theorem.

Theorem 3.4.1. A necessary and sufficient condition that $E_{3,2k+6}^3$ possess property T_3 is that $1 + y^4$ and $1 + 2y^2 + 2y^4$ be even

powers of y for some primitive element y of $\text{GF}(3^{2k+1})$.

Proof. Let us define a_1, a_2, \dots, a_7 as follows:

$$1 + 2y^2 = y^{a_1} \quad ,$$

$$1 + 2y^4 = y^{a_2} \quad ,$$

$$1 + y^2 + y^4 = y^{a_3} \quad ,$$

$$2 + 2y^2 = y^{a_4} \quad ,$$

$$2 + 2y^4 = y^{a_5} \quad ,$$

$$1 + y^2 + 2y^4 = y^{a_6} \quad ,$$

$$2 + y^2 + y^4 = y^{a_7} \quad .$$

For z the primitive element of $\text{GF}(3^4)$ with characteristic polynomial $z^4 - 2z^3 - 2z^2 - z - 1$, we have:

$$1 + 2z^5 = z^{58} \quad ,$$

$$1 + 2z^{10} = z^{20} \quad ,$$

$$1 + z^5 + z^{10} = z^{36} \quad ,$$

$$2 + 2z^5 = z^2 \quad ,$$

$$2 + 2z^{10} = z^{30} \quad ,$$

$$1 + z^5 + 2z^{10} = z^{51} \quad ,$$

$$2 + z^5 + z^{10} = z^{19} \quad .$$

Thus, (3.34) - (3.51) become, for the matrix $E_{3,2k+6}^3$,

$$(3.34') \quad \alpha_i = (y^{2i}, z^{5i}, 1) \quad ,$$

$$(3.35') \quad 2\alpha_i + 2\alpha_{i+1} = (y^{2i+a_4}, z^{5i+2}, 1),$$

$$(3.36') \quad 2\alpha_i + 2\alpha_{i+2} = (y^{2i+a_5}, z^{5i+30}, 1),$$

$$(3.37') \quad \alpha_i + \alpha_{i+1} + 2\alpha_{i+2} = (y^{2i+a_6}, z^{5i+51}, 1),$$

$$(3.38') \quad \alpha_i + 2\alpha_{i+1} + \alpha_{i+2} = (y^{2i+2a_4}, z^{5i+4}, 1),$$

$$(3.39') \quad 2\alpha_i + \alpha_{i+1} + \alpha_{i+2} = (y^{2i+a_7}, z^{5i+19}, 1),$$

$$(3.40') \quad 2\alpha_i = (y^{2i+(3^{2k+1}-1)/2}, z^{5i+40}, 2),$$

$$(3.41') \quad \alpha_i + \alpha_{i+1} = (y^{2i+a_4+(3^{2k+1}-1)/2}, z^{5i+42}, 2),$$

$$(3.42') \quad \alpha_i + \alpha_{i+2} = (y^{2i+a_5+(3^{2k+1}-1)/2}, z^{5i+70}, 2),$$

$$(3.43') \quad 2\alpha_i + 2\alpha_{i+1} + \alpha_{i+2} = (y^{2i+a_6+(3^{2k+1}-1)/2}, z^{5i+111}, 2),$$

$$(3.44') \quad 2\alpha_i + \alpha_{i+1} + 2\alpha_{i+2} = (y^{2i+2a_4+(3^{2k+1}-1)/2}, z^{5i+44}, 2),$$

$$(3.45') \quad \alpha_i + 2\alpha_{i+1} + 2\alpha_{i+2} = (y^{2i+a_7+(3^{2k+1}-1)/2}, z^{5i+59}, 2),$$

$$(3.46') \quad \alpha_i + 2\alpha_{i+1} = (y^{2i+a_1}, z^{5i+58}, 0),$$

$$(3.47') \quad \alpha_i + 2\alpha_{i+2} = (y^{2i+a_2}, z^{5i+20}, 0),$$

$$(3.48') \quad 2\alpha_i + \alpha_{i+1} = (y^{2i+a_1+(3^{2k+1}-1)/2}, z^{5i+18}, 0),$$

$$(3.49') \quad 2\alpha_i + \alpha_{i+2} = (y^{2i+a_2+(3^{2k+1}-1)/2}, z^{5i+60}, 0),$$

$$(3.50') \quad \alpha_i + \alpha_{i+1} + \alpha_{i+2} = (y^{2i+a_3}, z^{5i+36}, 0) ,$$

$$(3.51') \quad 2\alpha_i + 2\alpha_{i+1} + 2\alpha_{i+2} = (y^{2i+a_3+(3^{2k+1}-1)/2}, z^{5i+76}, 0) ,$$

for $i = 0, 1, \dots, 8(3^{2k+1} - 1) - 1$.

First of all the vectors in each vector set are distinct since $(y^{2i}, z^{5i}), i = 0, \dots, 8(3^{2k+1} - 1) - 1$, form a cycle of length $8(3^{2k+1} - 1)$. Secondly, the vector sets (3.46') - (3.51') are distinct because the vectors $(2i + a_1, 5i + 58), (2i + a_1 + (3^{2k+1}-1)/2, 5i + 18), (2i + a_2 + (3^{2k+1}-1)/2, 5i + 60), (2i + a_2 + (3^{2k+1}-1)/2, 5i + 60), (2i + a_3, 5i + 36)$, and $(2i + a_3 + (3^{2k+1}-1)/2, 5i + 76)$ are distinct vectors where the first component is reduced mod 2 and the second component is reduced mod 5. This follows because $(3^{2k+1}-1)/2$ is odd. We next note that the three collections of vector sets (3.34') - (3.39'), (3.40') - (3.45') and (3.46') - (3.51') are distinct since they differ in their last position. Now if the vector sets (3.34') - (3.39') are distinct, then so are the vector sets (3.40') - (3.45'), and conversely. Thus, a necessary and sufficient condition that $E_{3,2k+6}^3$ possess property T_3 is that $(0,0), (a_4,2), (a_5,30), (a_6,51), (2a_4,4), (a_7,19)$ be distinct, where the first component is reduced mod 2 and the second component is reduced mod 5. These vectors will be distinct if and only if a_5 and a_7 are odd, and a_5 and a_7 will be odd if and only if $1 + y^4$ and $1 + 2y^2 + 2y^4$ are even powers of y .

The efficiency of these codes is given as follows.

Theorem 3.4.2. Let f_{2k+6} be the efficiency of the code represented by $E_{3,2k+6}^3$. Then

$$(i) \quad f_{2k+6} = \frac{16(3^{2k+1} - 1)}{(3^{2k+4} - 1)}, \quad ,$$

$$(ii) \quad f_{2(k+1)+6} > f_{2k+6} \quad ,$$

$$(iii) \quad \lim_{k \rightarrow \infty} f_{2k+6} = 16/27 \quad .$$

The proof is immediate.

We note that $E_{3,2k+6}^3 = E_{3,2k+6}^3 \begin{bmatrix} 8(3^{2k+1} - 1)x(2k + 6) \\ \vdots \\ 1 \end{bmatrix}$ since y^{2i} is equivalent to the $(2k+1)$ -vector, with elements from $GF(3)$, which is the coefficient vector of the $2k$ -th degree polynomial in y representing y^{2i} , and, similarly, z^{5i} is equivalent to the 4-vector, with elements from $GF(3)$, which is the coefficient vector of the 3-rd degree polynomial in z representing z^{5i} . Finally, the last column is a column of ones.

Example 3.4.1. Let $k = 1$, and let y be that primitive element of $GF(3^3)$ which has $y^3 - y - 2$ as its characteristic polynomial.

Then $E_{3,8}^3$ is given as

$$E_{3,8}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y^2 & z^5 & 1 \\ \vdots & \vdots & \vdots \\ y^{414} & z^{1035} & 1 \end{bmatrix} = \begin{bmatrix} 100 & 1000 & 1 \\ 001 & 2020 & 1 \\ \vdots & \vdots & \vdots \\ 102 & 1121 & 1 \end{bmatrix}$$

where we note $y^{26} = z^{80} = 1$, and the equivalence between the non-zero elements of $GF(3^m)$ and the non-zero m -vectors over $GF(3)$. We have

$1 + y^4 = y^{18}$, and $1 + 2y^2 + 2y^4 = y^6$, so that, by Theorem 3.4.1, $E_{3,8}^3$ possesses property T_3 . Thus, by Theorem 1.2.1, $E_{3,8}^3$ represents an appropriate parity check matrix for the ternary linear code, $n = 208$, $r = 8$, which corrects all single error bursts of length less than or equal to 3. The efficiency of this code is $f_8 = 208/364 = .571$.

Example 3.4.2. Let $k = 2$, and let y be the primitive element of $GF(3^5)$ with characteristic polynomial $y^5 - y - 2$. Let $y' = y^5$ be a transformation of y to a new primitive element y' of $GF(3^5)$. Then $E_{3,10}^3$ is given as

$$E_{3,10}^3 = \begin{bmatrix} 1 & 1 & 1 \\ y'^2 & z^5 & 1 \\ \vdots & \vdots & \vdots \\ y'^{3870} & z^{9675} & 1 \end{bmatrix} .$$

We have $1 + y'^4 = y'^{102}$ and $1 + 2y'^2 + 2y'^4 = y'^{150}$, so that, by Theorem 3.4.1, $E_{3,10}^3$ possesses property T_3 . Thus, by Theorem 1.2.1, $E_{3,10}^3$ represents an appropriate parity check matrix for the ternary linear code, $n = 1936$, $r = 10$, which corrects all single error bursts of length less than or equal to 3. The efficiency of this code is $f_{10} = 1936/3280 = .591$.

CHAPTER IV

THE APPLICATION OF BOSE-CHAUDHURI CODES TO THE CONSTRUCTION OF BURST-ERROR-CORRECTING CODES

4.1. Introduction

Bose and Ray-Chaudhuri [6] have defined a class of binary group codes which has the property that if a message vector α of length $n = 2^m - 1$ is transmitted and if the received message vector β contains t or fewer errors, where t is a predetermined number and $m - t < n$, then the received message β is correctly decoded as α .

In this chapter we show that by augmenting the Bose-Chaudhuri parity check matrices defined in [6] the corresponding codes not only will possess the property of correcting t independent errors that may occur in the transmission of the messages of the code, but also will possess the property of correcting certain bursts of errors that may occur in transmission.

Bose and Ray-Chaudhuri proved in [6] that a necessary and sufficient condition that an (n, k) binary group code be t -error correcting is that the corresponding parity check matrix $D_t = D_t(n \times r)$ possess the property P_{2t} - the property that no set of $2t$ row vectors among the n row vectors in D_t be dependent. They then showed that if D_t is chosen as the matrix

$$D_t = \begin{bmatrix} 1 & 1 & \dots & 1 \\ y & y^3 & \dots & y^{2t-1} \\ y^2 & (y^2)^3 & \dots & (y^2)^{2t-1} \\ \dots & \dots & \dots & \dots \\ y^{2^m-2} & (y^{2^m-2})^3 & \dots & (y^{2^m-2})^{2t-1} \end{bmatrix}$$

where y is a primitive element of $GF(2^m)$, and where $(y^i)^j$, $i=0, 1, \dots, 2^m-2$; $j = 1, 3, 5, \dots, 2t-1$, is equivalent to the m -vector, with elements from $GF(2)$, which is the coefficient vector of the $(m-1)$ -th degree polynomial in y representing $(y^i)^j$, then D_t possesses property P_{2t} and hence the code corresponding to D_t is a t -error correcting binary group code.

To determine k , the number of information places, in any Bose-Chaudhuri (n, k) code, we note that $k = n - r$, where $r = R(m, t) = \text{rank } \underline{D}_t (n \times mt) \leq mt$. We note also that D_t can be regarded as an $n \times t$ matrix whose elements belong to $GF(2^m)$ or as an $n \times mt$ matrix whose elements belong to $GF(2)$. We shall regard D_t as the latter. Peterson [12] actually calculates $R(m, t)$ as follows: the rank $R(m, t)$ of D_t is the number of distinct residue classes mod n among the integers $2^j u$, $j = 0, 1, \dots, m-1$; $u=1, 3, \dots, 2t-1$. Since $R(m, t) \leq mt$, a lower bound on k is $n - mt$.

We show in Section 4.2 that if we augment $D_t = D_t(n \times mt)$ by adding a column of ones to D_t , the code corresponding to the augmented parity check matrix, say $D_t^* = D_t^* [n \times (mt + 1)]$, will correct all single bursts of errors of length $t + 1$ or less, as well as all t or fewer independent errors. We show also in Section 4.2 that, if $m \geq 4$ and is even, and $t = 2$, we can augment D_t in a particular way so as to obtain a two-error-correcting code which also corrects all single bursts of errors of length less than or equal to four, and with redundancy which does not exceed $2m + 3$.

In Section 4.3 we discuss briefly the multiple burst problem, i.e., how to construct an error-correcting code which will correct more than one error burst of length less than or equal to a pre-assigned number d . We show how to construct burst-error-correcting codes which correct the set of $(s + 1)$ independent bursts of errors of length less than or equal to two and which correct the set of $(s + 1)$ independent bursts of errors of length less than or equal to three. Again we use Bose-Chaudhuri codes which are augmented.

In Section 4.4 we mention unsolved problems in the construction of burst-error-correcting codes and some techniques that may be applicable to their solution.

4.2 Augmented Bose-Chaudhuri Codes Which Correct Single Bursts of Errors

Definition 4.2.1. We say that an (n, k) binary group code

is an augmented Bose-Chaudhuri code if the parity check matrix for this code is obtained from the Bose-Chaudhuri parity check matrix by adding one or more columns.

Lemma 4.2.1. Let D_t be the following Bose-Chaudhuri matrix:

$$D_t = \begin{bmatrix} 1 & 1 & \cdot & \cdot & \cdot & 1 \\ y & y^3 & \cdot & \cdot & \cdot & y^{2t-1} \\ y^2 & (y^2)^3 & \cdot & \cdot & \cdot & (y^2)^{2t-1} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ y^{2^m-2} & (y^{2^m-2})^3 & \cdot & \cdot & \cdot & (y^{2^m-2})^{2t-1} \end{bmatrix}$$

where y is a primitive element of $GF(2^m)$. Suppose that $t < 2^{m-1}$ (or, equivalently, $2t-1 < 2^m-1$). Then D_t^* has rank $R(m, t) + 1$, where

$$D_t^* = \begin{bmatrix} 1 & 1 & \cdot & \cdot & \cdot & 1 & 1 \\ y & y^3 & \cdot & \cdot & \cdot & y^{2t-1} & 1 \\ y^2 & (y^2)^3 & \cdot & \cdot & \cdot & (y^2)^{2t-1} & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ y^{2^m-2} & (y^{2^m-2})^3 & \cdot & \cdot & \cdot & (y^{2^m-2})^{2t-1} & 1 \end{bmatrix},$$

$1, y, y^3, \dots, y^{2t-1}$, each root y^i is the root of a unique irreducible polynomial $p_i(X)$ which divides $X^n - 1$, $i = 1, 3, 5, \dots, 2t-1$, and of course is a root of $1 + X$. Denoting by $p(X)$ the polynomial that generates the ideal, we can take $p(X)$ without loss of generality as

$$p(X) = \text{l.c.m.}_{i=1,3,5,\dots,2t-1} \{1 + X, p_i(X)\} .$$

Since each of the bracketed polynomials is irreducible, the l.c.m. is just their product with duplicates omitted. We note that duplications are possible, and should y^i and y^j , $i \neq j$, be roots of the same irreducible polynomial, the corresponding columns in D_t^* will be dependent. The only possible root of $1 + X$ is 1 , for if y^i were a root of $1 + X$, then $1 + y^i = 0$ which implies $y^i = 1$, contradicting the hypothesis that $i < 2^m - 1$, $i=1,3,5,\dots, 2t-1$. Now, using (2), we note that if $p(X)$ has degree r , the vector space of code words has rank $n-r$, and hence that the parity check matrix D_t^* has rank r . Now D_t has rank $R(m, t)$, and this rank is obtained in the same way as we obtain the rank of D_t^* (see Peterson [12]), but with $1 + X$ not included among the irreducible polynomials that generate the vector space of code words. Hence, $R(m, t) = r-1$, and this completes the proof.

Abramson [1] showed that by adding a column of ones to the Hamming code parity check matrix, a code is obtained which corrects all single bursts of length less than or equal to t as well as

all single errors. We prove, analogously, the following theorem for the Bose-Chaudhuri code parity check matrix.

Theorem 4.2.1. Let $D_t^* = D_t^* [n \times (mt + 1)]$ be the following matrix:

$$D_t^* = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ y & y^3 & \dots & y^{2t-1} & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ y^{2^m-2} & (y^{2^m-2})^3 & \dots & (y^{2^m-2})^{2t-1} & 1 \end{bmatrix},$$

where y is a primitive element of $GF(2^m)$, and where $2t-1 < 2^m-1$. Then the code corresponding to D_t^* corrects all single bursts of errors of length $t + 1$ or less, as well as all sets of t independent errors.

Proof. Since D_t^* possesses property P_{2t} , the code corresponding to D_t^* will correct all sets of t independent errors. Now let δ_i denote the i -th row vector of D_t^* , $i=0,1,\dots,2^m-2$ and let $\delta_{i_1}, \dots, \delta_{i_\ell}$ be any $\ell (\ell \leq t-1)$ vectors chosen from among $\delta_0, \delta_1, \dots, \delta_{2^m-2}$. Then, since D_t^* possesses property P_{2t} , it follows that

$$\delta_{i_1} + \dots + \delta_{i_\ell} \neq \delta_s + a_{s+1} \delta_{s+1} + \dots + a_{s+t-1} \delta_{s+t-1} + \delta_{s+t},$$

where $a_{s+\mu} \in GF(2)$, $\mu = 1, \dots, t-1$. That is, no set of $t-1$ or fewer independent errors can be confused with any burst sequence of

length $t + 1$. Next, let $\delta_{j_1}, \dots, \delta_{j_t}$ be any t vectors chosen from among $\delta_0, \dots, \delta_{2^m-2}$. Then

$$(4.1) \quad \delta_{j_1} + \dots + \delta_{j_t} + \delta_v + \delta_{v+1} + \dots + \delta_{v+t} \neq 0$$

since there are $(2t + 1)$ terms in the left hand member of (4.1) and each vector of D_t^* has a unity in its last position, thus ensuring that the sum shown in (4.1) has a one in its last position. Thus, we have

$$\delta_{j_1} + \dots + \delta_{j_t} \neq \delta_v + \dots + \delta_{v+t}.$$

Hence, no single burst of length $t+1$ can be confused with any set of t independent errors. Finally, it is clear by the nature of D_t^* that no two single bursts of length $t + 1$ can be confused.

This completes the proof.

Example 4.2.1. Suppose $t = 2$; then the matrix

$D_2^* = D_2^* [n \times (2m + 1)]$, where we write

$$D_2^* = \begin{bmatrix} 1 & 1 & 1 \\ y & y^3 & 1 \\ y^2 & (y^2)^3 & 1 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ y^{2^m-2} & (y^{2^m-2})^3 & 1 \end{bmatrix}$$

is an appropriate parity check matrix for the binary group code,

$n = 2^m - 1$, $r = R(m, 2) + 1$, which corrects all independent double errors as well as all single bursts of length less than or equal to three, for $m \geq 3$.

Now choose $m = 4$; then we have

$$D_2^* = \begin{bmatrix} 1 & 1 & 1 \\ y & y^3 & 1 \\ y^2 & (y^2)^3 & 1 \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ y^{14} & (y^{14})^3 & 1 \end{bmatrix} = \begin{bmatrix} 1000 & 1000 & 1 \\ 0100 & 0001 & 1 \\ 0010 & 0011 & 1 \\ \dots & \dots & \cdot \\ \dots & \dots & \cdot \\ \dots & \dots & \cdot \\ 1001 & 1111 & 1 \end{bmatrix}$$

choosing $y^4 + y + 1$ as the characteristic polynomial for y . Hence D_2^* is an appropriate parity check matrix for the binary group code, $n = 15$, $r = 9$, which corrects all independent double errors as well as all single bursts of errors of length 3 or less.

Example 4.2.2. Suppose $t = 3$; then the matrix

$$D_3^* = D_3^* \lfloor n \times (3m + 1) \rfloor, \text{ where we write}$$

$$D_3^* = \begin{bmatrix} 1 & 1 & 1 & 1 \\ y & y^3 & y^5 & 1 \\ y^2 & (y^2)^3 & (y^2)^5 & 1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ y^{2^m-2} & (y^{2^m-2})^3 & (y^{2^m-2})^5 & 1 \end{bmatrix},$$

is an appropriate parity check matrix for the binary group code, $n = 2^m - 1$, $r = R(m, 3) + 1$, which corrects all independent triple errors as well as all single bursts of length less than or equal to four, for $m \geq 3$.

Now choose $m = 5$; then we have

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ y & y^3 & y^5 & 1 \\ y^2 & (y^2)^3 & (y^2)^5 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ y^{30} & (y^{30})^3 & (y^{30})^5 & 1 \end{bmatrix} =$$

$$\begin{bmatrix} 10000 & 10000 & 10000 & 1 \\ 01000 & 00010 & 10100 & 1 \\ 00100 & 000010 & 10001 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ 01001 & 01101 & 11101 & 1 \end{bmatrix}$$

choosing $y^5 + y^2 + 1$ as the characteristic polynomial for y . Hence D_3^* is an appropriate parity check matrix for the binary group code, $n = 31$, $r = R(5, 3) + 1$, which corrects all independent triple errors as well as all single bursts of errors of length 4 or less. We determine $R(5, 3)$ as follows: $R(5, 3)$ is

the number of distinct residue classes mod 31 among the integers

$2^j u$, $j = 0, 1, 2, 3, 4$; $u = 1, 3, 5$. The classes are:

1	2	4	8	16
3	6	12	24	17
5	10	20	9	18

Thus, $r = 16$.

We now show that we can augment the parity check matrix for the two-error-correcting Bose-Chaudhuri code in such a way that we obtain a parity check matrix for a two-error-correcting code which also corrects all single bursts of length less than or equal to four. We shall first need the following lemma.

Lemma 4.2.2. Let $m \geq 4$ be even, and let $D_m^{**} = D_m^{**}(nx2m+3)$

be the following matrix:

$$(4.2) \quad D_m^{**} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ y & y^3 & z & 1 \\ y^2 & (y^2)^3 & z^2 & 1 \\ \vdots & \vdots & \vdots & \vdots \\ y^{2^m-4} & (y^{2^m-4})^3 & 1 & 1 \\ y^{2^m-3} & (y^{2^m-3})^3 & z & 1 \\ y^{2^m-2} & (y^{2^m-2})^3 & z^2 & 1 \end{bmatrix},$$

where y is a primitive element of $GF(2^m)$, z is a primitive element of $GF(2^2)$, and the last column is a column of ones. Then D_m^{**} has rank $R(m, 2) + 3$, where D_2 has rank $R(m, 2)$.

The proof of Lemma 4.2.2 is analogous to that of Lemma 4.2.1 and so is omitted.

Theorem 4.2.2. Let D_m^{**} be the matrix (4.2) and let m be even, $m \geq 4$. Suppose, further, that y can be chosen so that $1 + y + y^2 + y^3 + y^4 = y^\theta$, $\theta \not\equiv 2 \pmod{3}$, and that one of the three following conditions holds:

$$(i) \quad \frac{1 + y^2 + y^3}{1 + y + y^3} = y^\phi, \quad \phi \not\equiv 1 \pmod{3};$$

$$(ii) \quad \frac{1 + y^6 + y^9}{1 + y^3 + y^9} = y^\lambda, \quad \lambda \not\equiv 0 \pmod{3};$$

$$(iii) \quad y^{16} + y^{13} + y^{11} + y^5 + y^3 + 1 \neq 0.$$

Then D_m^{**} will be an appropriate parity check matrix for the binary group code, $n = 2^m - 1$, $r = R(m, 2) + 3$, which corrects all independent double errors and all single bursts of errors of length less than or equal to four.

Proof. Let δ_i be the i -th row vector of D_m^{**} , $i = 0, 1, \dots, 2^m - 2$, and let δ_{i_1} and δ_{i_2} be any two distinct vectors chosen from the vectors $\delta_0, \delta_1, \dots, \delta_{2^m - 2}$. Then by virtue of property P_4 possessed by D_m^{**} , we need prove only the following:

$$(4.3) \quad \delta_{i_1} + \delta_{i_2} \neq \delta_v + \delta_{v+1} + \delta_{v+2},$$

$$(4.4) \quad \delta_{i_1} + \delta_{i_2} \neq \delta_v + \delta_{v+1} + \delta_{v+3},$$

$$(4.5) \quad \delta_{i_1} + \delta_{i_2} \neq \delta_v + \delta_{v+2} + \delta_{v+3},$$

$$v = 0, 1, \dots, 2^m - 2;$$

$$(4.6) \quad \delta_v + \delta_{v+1} + \delta_{v+2} \neq \delta_j + \delta_{j+1} + \delta_{j+2} + \delta_{j+3},$$

$$(4.7) \quad \delta_v + \delta_{v+1} + \delta_{v+3} \neq \delta_j + \delta_{j+1} + \delta_{j+2} + \delta_{j+3},$$

$$(4.8) \quad \delta_v + \delta_{v+2} + \delta_{v+3} \neq \delta_j + \delta_{j+1} + \delta_{j+2} + \delta_{j+3},$$

$$(4.9) \quad \delta_v = \delta_j + \delta_{j+1} + \delta_{j+2} + \delta_{j+3},$$

$$(4.10) \quad \delta_{i_1} + \delta_{i_2} \neq \delta_v + \delta_{v+1} + \delta_{v+2} + \delta_{v+3},$$

$$(4.11) \quad \delta_v + \delta_{v+1} + \delta_{v+3} \neq \delta_j + \delta_{j+2} + \delta_{j+3},$$

$$(4.12) \quad \delta_v + \delta_{v+2} + \delta_{v+3} \neq \delta_j + \delta_{j+1} + \delta_{j+2},$$

$$(4.13) \quad \delta_v + \delta_{v+1} + \delta_{v+3} \neq \delta_j + \delta_{j+1} + \delta_{j+2},$$

For $v \neq j$, $v, j = 0, 1, \dots, 2^m - 2$. For if (4.3) - (4.13) are all satisfied it then follows from Corollary 1.1.1 that D_m^{**} will be an appropriate parity check matrix for the binary group code, $n = 2^m - 1$, $r = R(m, 2) + 3$, which corrects all independent double errors and all single bursts of errors of length less than or equal to four.

(4.3) - (4.9) obviously hold since each of these statements has an odd number of terms on one side and an even number of terms on the other side. Now let

$$\begin{aligned}
1 + y + y^2 &= y^{a_1}, & 1 + y^3 + y^6 &= y^{a_2}, \\
1 + y + y^3 &= y^{b_1}, & 1 + y^3 + y^9 &= y^{b_2}, \\
1 + y^2 + y^3 &= y^{c_1}, & 1 + y^6 + y^9 &= y^{c_2}.
\end{aligned}$$

Then (4.12) and (4.13) both hold, because

$$\begin{aligned}
\delta_i + \delta_{i+1} + \delta_{i+2} &= (y^{i+a_1}, y^{3i+a_2}, 0, 1), \\
\delta_i + \delta_{i+1} + \delta_{i+3} &= (y^{i+b_1}, y^{3i+b_2}, z^{i+1}, 1), \\
\delta_i + \delta_{i+2} + \delta_{i+3} &= (y^{i+c_1}, y^{3i+c_2}, z^{i+2}, 1),
\end{aligned}$$

$i = 0, 1, \dots, 2^m - 2$, and hence in both (4.12) and (4.13) the two members differ in the third position. Thus it remains only to prove that (4.10) and (4.11) hold.

Suppose that (4.10) does not hold. Then there exist $\delta_{i_1}, \delta_{i_2}$ δ_v such that

$$\delta_{i_1} + \delta_{i_2} = \delta_v + \delta_{v+1} + \delta_{v+2} + \delta_{v+3},$$

or, equivalently,

$$(4.14) \quad y^{i_1} + y^{i_2} = y^v (1 + y)^3,$$

$$(4.15) \quad y^{3i_1} + y^{3i_2} = y^{3v} (1 + y^3)^3,$$

$$(4.16) \quad z^{i_1} + z^{i_2} = z^v$$

hold simultaneously. Now let $i'_1 = i_1 - v$ and $i'_2 = i_2 - v$; then

(4.14) - (4.16) become

$$(4.14') \quad y^{i'_1} + y^{i'_2} = (1+y)^3,$$

$$(4.15') \quad y^{3i'_1} + y^{3i'_2} = (1 + y^3)^3,$$

$$(4.16') \quad z^{i'_1} + z^{i'_2} = 1.$$

Dividing (4.14') into (4.15'), we get

$$(4.17) \quad y^{2i'_1} + y^{2i'_2} + y^{i'_1 + i'_2} = (1 + y + y^2)^3 = 1 + y + y^3 + y^5 + y^6,$$

and by squaring (4.14') we obtain

$$(4.18) \quad y^{2i'_1} + y^{2i'_2} = (1 + y)^6 = 1 + y^2 + y^4 + y^6.$$

Thus, adding (4.17) and (4.18), we have

$$(4.19) \quad y^{i'_1 + i'_2} = y + y^2 + y^3 + y^4 + y^5.$$

Now $z^{i'_1} + z^{i'_2} = 1$ implies $i'_1 + i'_2 = 0 \pmod{3}$, but by hypothesis $1 + y + y^2 + y^3 + y^4 = y^\theta$, where $\theta \not\equiv 2 \pmod{3}$, whence by (4.19), $i'_1 + i'_2 = 1 + \theta \not\equiv 0 \pmod{3}$. This is a contradiction and hence establishes (4.10).

Finally, if (4.11) does not hold, then there exist i and j such that

$$\delta_i + \delta_{i+1} + \delta_{i+3} = \delta_j + \delta_{j+2} + \delta_{j+3},$$

or, equivalently,

$$(4.20) \quad y^i (1 + y + y^3) = y^j (1 + y^2 + y^3),$$

$$(4.21) \quad y^{3i} (1 + y^3 + y^9) = y^{3j} (1 + y^6 + y^9),$$

$$(4.22) \quad z^{i+1} = z^{j+2}$$

hold simultaneously. Now set $i' = i - j$. Then (4.20) - (4.22)

become

$$(4.20') \quad y^{i'} (1 + y + y^3) = (1 + y^2 + y^3),$$

$$(4.21') \quad y^{3i'}(1 + y^3 + y^9) = (1 + y^6 + y^9),$$

$$(4.22') \quad z^{i'} = z.$$

From (4.20') and (4.21') we get

$$(4.23) \quad (1+y+y^3)(1+y^2+y^6)(1+y^6+y^9) = (1+y^2+y^3)(1+y^4+y^6)(1+y^3+y^9),$$

or, equivalently,

$$(4.24) \quad y^{16} + y^{13} + y^{11} + y^5 + y^3 + 1 = 0.$$

Also, (4.20') gives

$$y^{i'} = y^{\phi},$$

while (4.22') gives $i' = 1 \pmod{3}$, so that $\phi = 1 \pmod{3}$. Finally,

(4.21') gives

$$y^{3i'} = y^{\lambda},$$

whence $\lambda = 0 \pmod{3}$. Hence, none of the conditions (i), (ii),

(iii) of the hypothesis is satisfied, which gives us a contradiction.

This establishes 4.11 and completes the proof of the theorem.

Example 4.2.3. Suppose $m = 4$, then D_4^{**} is the following matrix:

$$D_4^{**} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ y & y^3 & z & 1 \\ y^2 & (y^2)^3 & z^2 & 1 \\ y^3 & (y^3)^3 & 1 & 1 \\ y^4 & (y^4)^3 & z & 1 \\ y^5 & (y^5)^3 & z^2 & 1 \\ y^6 & (y^6)^3 & 1 & 1 \\ y^7 & (y^7)^3 & z & 1 \\ y^8 & (y^8)^3 & z^2 & 1 \\ y^9 & (y^9)^3 & 1 & 1 \\ y^{10} & (y^{10})^3 & z & 1 \\ y^{11} & (y^{11})^3 & z^2 & 1 \\ y^{12} & (y^{12})^3 & 1 & 1 \\ y^{13} & (y^{13})^3 & z & 1 \\ y^{14} & (y^{14})^3 & z^2 & 1 \end{bmatrix} = \begin{bmatrix} 1000 & 1000 & 10 & 1 \\ 0100 & 0001 & 01 & 1 \\ 0010 & 0011 & 11 & 1 \\ 0001 & 0101 & 10 & 1 \\ 1100 & 1111 & 01 & 1 \\ 0110 & 1000 & 11 & 1 \\ 0011 & 0001 & 10 & 1 \\ 1101 & 0011 & 01 & 1 \\ 1010 & 0101 & 11 & 1 \\ 0101 & 1111 & 10 & 1 \\ 1110 & 1000 & 01 & 1 \\ 0111 & 0001 & 11 & 1 \\ 1111 & 0011 & 10 & 1 \\ 1011 & 0101 & 01 & 1 \\ 1001 & 1111 & 11 & 1 \end{bmatrix}$$

where y is chosen to be the primitive element of $GF(2^4)$ with characteristic polynomial $y^4 + y + 1$. Now,

$$1 + y + y^2 + y^3 + y^4 = y^6, \quad 6 \not\equiv 2 \pmod{3};$$

and

$$\frac{1 + y^2 + y^3}{1 + y + y^3} = \frac{y^{13}}{y^7} = y^6, \quad 6 \neq 1 \pmod{3}$$

Hence, by Theorem 4.2.2, D_4^{**} is an appropriate parity check matrix for the binary group code, $n = 15$, $r = 11$, which corrects all independent double errors as well as all bursts of length less than or equal to four. We note that $r = 11$ since $R(4,2) = 8$.

Example 4.2.4. Suppose $m = 6$, and let D_6^{**} be the following matrix:

$$D_6^{**} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ y' & y'^3 & z & 1 \\ y'^2 & (y'^3)^2 & z^2 & 1 \\ \hline \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \hline y'^{60} & (y'^{60})^3 & 1 & 1 \\ y'^{61} & (y'^{61})^3 & z & 1 \\ y'^{62} & (y'^{62})^3 & z^2 & 1 \end{bmatrix} = \begin{bmatrix} 100000 & 100000 & 10 & 1 \\ 000001 & 000101 & 01 & 1 \\ 000011 & 110011 & 11 & 1 \\ \hline \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \hline 101100 & 111100 & 10 & 1 \\ 010101 & 010010 & 01 & 1 \\ 111111 & 101100 & 11 & 1 \end{bmatrix}$$

where we chose y to be the primitive element of $GF(2^6)$ with characteristic polynomial $y^6 + y + 1$, and y' is another primitive element of $GF(2^6)$, obtained from y by using the transformation $y' = y^5$. Now

$$1 + y' + y'^2 + y'^3 + y'^4 = y'^{15}, \quad 15 \not\equiv 2 \pmod{3};$$

and

$$\frac{1 + y'^2 + y'^3}{1 + y' + y'^3} = y'^{53}, \quad 53 \not\equiv 1 \pmod{3}.$$

Hence, by Theorem 4.2.2, D_4^{**} is an appropriate parity check matrix for the binary group code, $n = 63$, $r = R(6, 2) + 3$, which corrects all independent double errors as well as all single bursts of length less than or equal to four. Now $R(6, 2)$ is the number of distinct residue classes mod 63 among the integers $2^j u$, $j = 0, 1, \dots, 5$; $u = 1, 3$. These classes are:

1	2	4	8	16	32
3	6	12	24	48	33

Hence, $R(6, 2) = 12$, which yields $r = 15$.

4.3. Augmented Bose-Chaudhuri Codes Useful in Correcting Multiple Bursts of Errors

In this section we obtain augmented Bose-Chaudhuri codes which correct multiple bursts of errors of length 2 and 3.

Theorem 4.3.1. Consider the following augmented Bose-Chaudhuri matrix $A_{2s+1} = A_{2s+1} (n \times \lfloor (2s+1)m + \underline{1} \rfloor)$

$$A_{2s+1} = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ y & y^3 & \dots & y^{4s+1} & 1 \\ y^2 & (y^2)^3 & \dots & (y^2)^{4s+1} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ y^{2^m-2} & (y^{2^m-2})^3 & \dots & (y^{2^m-2})^{4s+1} & 1 \end{bmatrix}$$

where y is a primitive element of $GF(2^m)$. Then A_{2s+1} is an appropriate parity check matrix for the binary group code, $n = 2^m - 1$, $r = R(m, 2s + 1) + 1$, which corrects a set of $(s + 1)$ independent bursts of errors of length less than or equal to two, as well as all $(2s + 1)$ independent errors, provided that $2^m - 1 > 4s + 1$, $s \geq 1$.

Proof. Let δ_i denote the i -th row vector of A_{2s+1} , $i = 0, 1, \dots, 2^m - 2$. First of all, A_{2s+1} possesses property P_{4s+2} , and thus the set of all $(2s + 1)$ independent errors are corrected; that is, if $\delta_{i_1}, \dots, \delta_{i_\ell}$ are any ℓ vectors from $\delta_0, \delta_1, \dots, \delta_{2^m-2}$, with $\ell \leq 4s + 2$, then $\delta_{i_1} + \dots + \delta_{i_\ell} \neq 0$. Hence, to complete the proof of the theorem we need only show the following:

$$(4.25) \delta_{i_1} + \delta_{i_2} + \dots + \delta_{i_{2s+1}} \neq (\delta_{i'_1} + \delta_{i'_1+1}) + \dots + (\delta_{i'_{s+1}} + \delta_{i'_{s+1}+1}),$$

where $\delta_{i_1}, \dots, \delta_{i_{2s+1}}$; $\delta_{i'_1}, \dots, \delta_{i'_{s+1}}$ are any $3s + 2$ vectors chosen

from $\delta_0, \delta_1, \dots, \delta_{2^m-2}$; and

$$(4.26) \quad (\delta_{j_1} + \delta_{j_1+1}) + \dots + (\delta_{j_{s+1}} + \delta_{j_{s+1}+1}) \neq (\delta_{j'_1} + \delta_{j'_1+1}) + \dots \\ + (\delta_{j'_{s+1}} + \delta_{j'_{s+1}+1}),$$

where $\delta_{j_1}, \dots, \delta_{j_{s+1}}; \delta_{j'_1}, \dots, \delta_{j'_{s+1}}$ are any $2s+2$ vectors chosen from $\delta_0, \delta_1, \dots, \delta_{2^m-2}$. (4.25) is clearly satisfied since the resulting sum on the left-hand side of (4.25) contains a one in its last position, whereas the resulting sum on the right-hand side of (4.25) contains a zero in its last position. To show that (4.26) is satisfied, assume that for some set of vectors $\delta_{j_1}, \dots, \delta_{j_{s+1}}; \delta_{j'_1}, \dots, \delta_{j'_{s+1}}$,

$$(\delta_{j_1} + \delta_{j_1+1}) + \dots + (\delta_{j_{s+1}} + \delta_{j_{s+1}+1}) = (\delta_{j'_1} + \delta_{j'_1+1}) + \dots \\ + (\delta_{j'_{s+1}} + \delta_{j'_{s+1}+1}).$$

Then,

$$y^{j_1(1+y)} + \dots + y^{j_{s+1}(1+y)} = y^{j'_1(1+y)} + \dots + y^{j'_{s+1}(1+y)}, \\ y^{3j_1(1+y^3)} + \dots + y^{3j_{s+1}(1+y^3)} = y^{3j'_1(1+y^3)} + \dots + y^{3j'_{s+1}(1+y^3)}, \\ \vdots \\ y^{(4s+1)j_1(1+y^{4s+1})} + \dots + y^{(4s+1)j_{s+1}(1+y^{4s+1})} = \\ y^{(4s+1)j'_1(1+y^{4s+1})} + \dots + y^{(4s+1)j'_{s+1}(1+y^{4s+1})},$$

all hold simultaneously. Since $2^m - 1 > 4s + 1$, it follows that $1 + y^v \neq 0$ for $v = 1, 3, 5, \dots, 4s + 1$. Hence the above equations imply that

$$\begin{aligned} y^{j_1} + \dots + y^{j_{s+1}} &= y^{j'_1} + \dots + y^{j'_{s+1}}, \\ y^{3j_1} + \dots + y^{3j_{s+1}} &= y^{3j'_1} + \dots + y^{3j'_{s+1}}, \\ &\vdots \\ y^{(4s+1)j_1} + \dots + y^{(4s+1)j_{s+1}} &= y^{(4s+1)j'_1} + \dots + y^{(4s+1)j'_{s+1}} \end{aligned}$$

all hold simultaneously, or that

$$(4.27) \quad \delta_{j_1} + \dots + \delta_{j_{s+1}} = \delta_{j'_1} + \dots + \delta_{j'_{s+1}}.$$

This implies, however, that A_{2s+1} has at most property P_{2s+1} , which is a contradiction.

Example 4.3.1. If $s = 1$, then we obtain the same parity check matrix as in Example 4.2.2. Thus we note that this code not only corrects all independent triple errors and all single bursts of errors of length less than or equal to four, but also corrects all independent double bursts of errors of length less than or equal to two.

Example 4.3.2. If $s = 2$, then A_5 becomes

$$A_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ y & y^3 & y^5 & y^7 & y^9 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ y^{2^m-2} & (y^{2^m-2})^3 & (y^{2^m-2})^5 & (y^{2^m-2})^7 & (y^{2^m-2})^9 & 1 \end{bmatrix}$$

Thus, by Theorem 4.3.1, A_5 is an appropriate parity check matrix for the binary group code $n = 2^m - 1$, $r = R(m, 5) + 1$, which corrects all independent quintuple errors as well as all independent triple bursts of errors of length less than or equal to two, provided, $m \geq 4$.

Theorem 4.3.2. Consider the following augmented Bose-Chaudhuri matrix:

$$A_{3s+2} = \begin{bmatrix} 1 & 1 & \dots & 1 & 1 \\ y & y^3 & \dots & y^{6s+3} & 1 \\ y^2 & (y^2)^3 & \dots & (y^2)^{6s+3} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ y^{2^m-2} & (y^{2^m-2})^3 & \dots & (y^{2^m-2})^{6s+3} & 1 \end{bmatrix},$$

where y is a primitive element of $GF(2^m)$. Then A_{3s+2} is an appropriate parity check matrix for the binary group code, $n = 2^m - 1$, $r = R(m, 3s + 2) + 1$, which corrects the set of all independent $(s + 1)$ -bursts of errors of length less than or equal to three as well as the set of all $(3s + 2)$ independent errors, where $s \geq 1$ and $2^m - 1 > 6s + 3$.

Proof. Since A_{3s+2} possesses property P_{6s+4} , all the set of $(3s + 2)$ -independent errors are corrected. Hence, to complete the

proof of the theorem we need show only the following (letting δ_i be the i -th row vector of A_{3s+2} , $i = 0, 1, \dots, 2^m - 2$):

$$(4.28) \quad \delta_{i_1} + \dots + \delta_{i_{3s+2}} \neq (\delta_{i'_1} + \delta_{i'_1+1} + \delta_{i'_1+2}) + \dots \\ + (\delta_{i'_{s+1}} + \delta_{i'_{s+1}+1} + \delta_{i'_{s+1}+2}) ,$$

where $\delta_{i_1}, \dots, \delta_{i_{3s+2}}$; $\delta_{i'_1}, \dots, \delta_{i'_{s+1}}$ are any $4s + 3$ vectors

chosen from $\delta_0, \delta_1, \dots, \delta_{2^m-2}$; and

$$(4.29) \quad (\delta_{j_1} + \delta_{j_1+1} + \delta_{j_2+2}) + \dots + (\delta_{j_{s+1}} + \delta_{j_{s+1}+1} + \delta_{j_{s+1}+2}) \\ \neq (\delta_{j'_1} + \delta_{j'_1+1} + \delta_{j'_1+2}) + \dots + \\ (\delta_{j'_{s+1}} + \delta_{j'_{s+1}+1} + \delta_{j'_{s+1}+2}) ,$$

where $\delta_{j_1}, \dots, \delta_{j_{s+1}}$; $\delta_{j'_1}, \dots, \delta_{j'_{s+1}}$ are any $2s + 2$ vector chosen

from $\delta_0, \delta_1, \dots, \delta_{2^m-2}$. (4.28) is clearly satisfied because the

resulting sum of the left-hand side of (4.28) and that of the right-

hand side of (4.28) differ in their last positions. To prove that

(4.29) holds, assume there exists a set of vectors $\delta_{i_1}, \dots, \delta_{i_{s+1}}$;

$\delta_{i'_1}, \dots, \delta_{i'_{s+1}}$ such that

bursts of errors of length less than or equal to three. Let

$A_{2s_1+1} = A_{3s_2+2}$ be the required parity check matrix, and let δ_i be the i -th row vector of A_{2s_1+1} , $i = 0, 1, \dots, 2^m - 2$. Now, if

$$\begin{aligned} & (\delta_{i_1} + \delta_{i_1+1}) + \dots + (\delta_{i_{s_1+1}} + \delta_{i_{s_1+1}+1}) = \\ & (\delta_{i_1'} + \delta_{i_1'+1} + \delta_{i_1'+2}) + \dots + (\delta_{i_{s_2+1}'} + \delta_{i_{s_2+1}'+1} \\ & \qquad \qquad \qquad + \delta_{i_{s_2+1}'+2}) \end{aligned}$$

for arbitrary vectors $\delta_{i_1}, \dots, \delta_{i_{s_1+1}}$; $\delta_{i_1'}, \dots, \delta_{i_{s_2+1}'}$, then

$$\begin{aligned} y^{vi_1}(1+y^v) + \dots + y^{vi_{s_1+1}}(1+y^v) &= y^{vi_1'}(1+y^v+y^{2v}) + \dots + \\ & y^{vi_{s_2+1}'}(1+y^v+y^{2v}) \end{aligned}$$

for $v = 1, 3, \dots, 4s_1 + 1 (= 6s_2 + 3)$. This, however, implies that

$$\begin{aligned} y^{vi_1}(1+y^{2v}) + \dots + y^{vi_{s_1+1}}(1+y^{2v}) &= y^{vi_1'}(1+y^{3v}) + \dots + \\ & y^{vi_{s_2+1}'}(1+y^{3v}) \end{aligned}$$

for $v = 1, 3, \dots, 4s_1 + 1 (= 6s_2 + 3)$, and thus that

$$\begin{aligned} (\delta_{i_1} + \delta_{i_1+2}) + \dots + (\delta_{i_{s_1+1}} + \delta_{i_{s_1+1}+2}) &= (\delta_{i_1'} + \delta_{i_1'+3}) + \dots + \\ & (\delta_{i_{s_2+1}'} + \delta_{i_{s_2+1}'+3}) \end{aligned}$$

which implies that $A_{2s_1+1} = A_{3s_1+2}$ has at most property P_{5s_2+4} , and

this contradicts that A_{3s_2+2} has property P_{6s_2+4} . Also,

$$(\delta_{i_1} + \delta_{i_1+1}) + \dots + (\delta_{i_{s_1}} + \delta_{i_{s_1}+1}) + \delta_{i_{s_1}} \neq$$

$$(\delta_{i'_1} + \delta_{i'_1+1} + \delta_{i'_1+2}) + \dots + (\delta_{i'_{s_2+1}} + \delta_{i'_{s_2+1}+1} + \delta_{i'_{s_2+1}+2}) ,$$

for there are $2s_1 + 1$ vectors in the sum on the left-hand side and $3s_2 + 3$ vectors in the sum on the right-hand side, while $3s_2 + 3 = 2s_1 + 2$, so that the two sums differ in their last positions.

Similarly,

$$(\delta_{i_1} + \delta_{i_1+1}) + \dots + (\delta_{i_{s_1+1}} + \delta_{i_{s_1+1}+1}) \neq (\delta_{i'_1} + \delta_{i'_1+1} + \delta_{i'_1+2})$$

$$+ \dots + (\delta_{i'_{s_2}} + \delta_{i'_{s_2}+1} + \delta_{i'_{s_2}+2}) + (\delta_{i'_{s_2+1}} + \delta_{i'_{s_2+1}+1})$$

and

$$(\delta_{i_1} + \delta_{i_1+1}) + \dots + (\delta_{i_{s_1+1}} + \delta_{i_{s_1+1}+1}) \neq (\delta_{i'_1} + \delta_{i'_1+1} + \delta_{i'_1+2})$$

$$+ \dots + (\delta_{i'_{s_2}} + \delta_{i'_{s_2}+1} + \delta_{i'_{s_2}+2}) + (\delta_{i'_{s_2+1}} + \delta_{i'_{s_2+1}+2}) .$$

Finally,

$$(\delta_{i_1} + \delta_{i_1+1}) + \dots + (\delta_{i_{s_1}} + \delta_{i_{s_1}+1}) + \delta_{i_{s_1}+1} \neq$$

$$(\delta_{i'_1} + \delta_{i'_1+1} + \delta_{i'_1+2}) + \dots + (\delta_{i'_{s_2}} + \delta_{i'_{s_2}+1} + \delta_{i'_{s_2}+2}) \\ + (\delta_{i'_{s_2}+1} + \delta_{i'_{s_2}+1+1})$$

because of property P_{4s_1+2} of the matrix A_{2s_1+1} . Similarly,

$$(\delta_{i_1} + \delta_{i_1+1}) + \dots + (\delta_{i_{s_1}} + \delta_{i_{s_1}+1}) + \delta_{i_{s_1}+1} \neq$$

$$(\delta_{i'_1} + \delta_{i'_1+1} + \delta_{i'_1+2}) + \dots + (\delta_{i'_{s_2}} + \delta_{i'_{s_2}+1} + \delta_{i'_{s_2}+2}) + \\ (\delta_{i'_{s_2}+1} + \delta_{i'_{s_2}+1+2}) .$$

4.4. Further Problems in the Construction of Multiple-Burst-Error-Correcting Codes.

The general problem in the construction of multiple-burst-error-correcting codes is to find a code that will correct with certainty the set of all independent s -bursts of errors, each of length less than or equal to d , in such a way that, for a given redundancy r , the number of places in each message, say n , is as large as possible. In this chapter we have discussed one particular method for obtaining multiple-burst-error-correcting codes for burst length less than or equal to three. There is one possible approach

different from the methods here that may be useful in constructing multiple-burst-error-correcting codes in the binary case. This method involves the examination of Bose-Chaudhuri codes which correct the set of all s independent errors for the 2^d -nary case. It is conjectured that a correspondence can be established so that such a Bose-Chaudhuri code can be made equivalent to a certain binary group code which will correct the set of all s independent bursts of length less than or equal to d . Thus, one extension of the work in this chapter is to investigate such codes.

BIBLIOGRAPHY

- [1] Abramson, N. M., "A class of systematic codes for non-independent errors," IRE Transactions, IT-5 (1959), pp. 150-157.
- [2] Albert, A. A., Fundamental Concepts of Higher Algebra, University of Chicago Press, Chicago, Ill. (1956), pp. 159-160.
- [3] Birkhoff, G. and MacLane, S., A Survey of Modern Algebra, Macmillan Co., New York, N. Y. (1941), pp. 427-456.
- [4] Bose, R. C., "On some connections between the design of experiments and information theory," Case Institute of Technology, Report No. 1022 (1960).
- [5] Bose, R. C. and Chakravarti, I. M., "Binary group codes with even redundancy which correct consecutive errors in bursts of three or less," (Abstract), American Mathematical Society Notices, Vol. 8 (1961) pp. 146-147.
- [6] Bose, R. C. and Ray-Chaudhuri, D. K., "On a class of error correcting binary group codes," Information and Control, Vol. 3 (1960), pp. 68-79.
- [7] Carmichael, R. D., Introduction to the Theory of Groups of Finite Order, Ginn and Company, Boston, Mass. (1937), pp. 242-288.
- [8] Elspas, B., "A note on p-nary adjacent error correcting codes," IRE Transactions, IT-6 (1960), pp. 13-15.

- [9] Gilbert, E. N., "A problem in binary coding," Proceedings of Symposium in Applied Mathematics, Combinatorial Analysis, 10 (1960), pp. 291-297.
- [10] Golay, M. J. F., "Notes on digital coding," Proceedings of the Institute of Radio Engineers, Vol. 37 (1949), p. 657.
- [11] Hamming, R. W., "Error detecting and error correcting codes," Bell Systems Technical Journal, Vol. 29 (1950), pp. 147-160.
- [12] Peterson, W. W., "Encoding and error-correction procedures for the Bose-Chaudhuri codes," IRE Transactions, IT-6 (1960), pp. 459-470.
- [13] Peterson, W. W., Error Correcting Codes, Massachusetts Institute of Technology Press and John Wiley and Sons, Inc., Cambridge, Mass. and New York, N. Y. (1961), p. 61.
- [14] Reiger, S. H., "Codes for the correction of 'clustered' errors," IRE Transactions, IT-6 (1960), pp. 16-21.