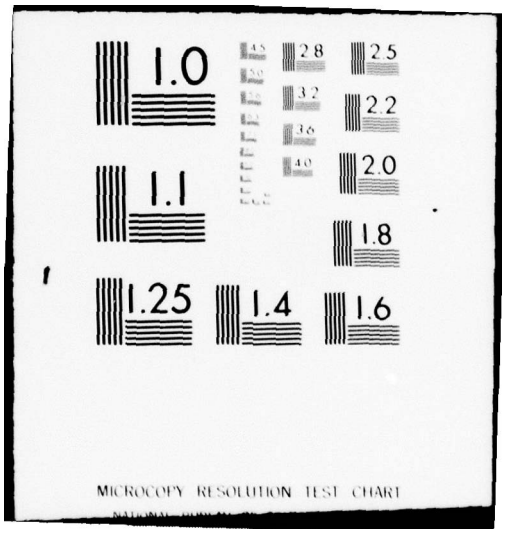
AD-A063 389 SOUTHERN METHODIST UNIV DALLAS TX DEPT OF COMPUTER S--ETC F/G 9/4
ON THE THEORY OF UNIDIRECTIONAL ERROR CORRECTING/DETECTING CODE--ETC(U)
SEP 78 B BOSE, T R RAO N00014-77-C-0455
UNCLASSIFIED CS-7817 NL

1 OF 1
AD A063389

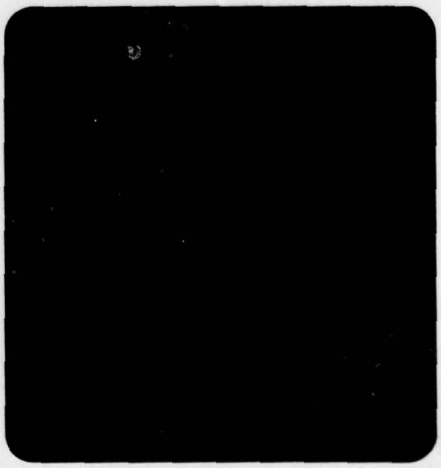
END
DATE FILMED
3-79
DDC


1.0
1.1
1.25
1.4
1.6
1.8
2.0
2.2
2.5
2.8
3.2
3.6
4.0
MICROCOPY RESOLUTION TEST CHART

12 B

LEVEL II

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING



SOUTHERN METHODIST UNIVERSITY
SCHOOL OF ENGINEERING
AND APPLIED SCIENCE
DALLAS, TEXAS 75275

(9) Technical Report CS 7817

(14) CS-7817

(6) ON THE THEORY OF UNIDIRECTIONAL ERROR CORRECTING/DETECTING CODES*

(10) Bella Bose
T.R.N. Rao

(12) 36p.

409158

Department of Computer Science
Southern Methodist University
Dallas, Texas 75275

(15) N00014-77-C-0455,
NSF-ENG76-11237

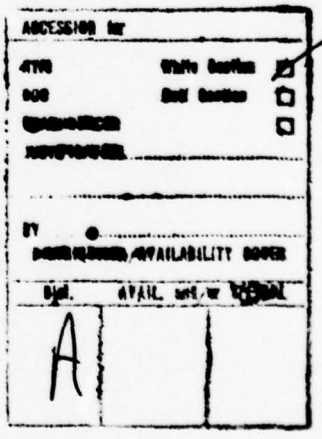
(11) September 1978

*Supported by NSF grant ENG 76-11237 and
ONR contract N00014-77-C-0455.

409158

ABSTRACT

In this report, we present some basic theory on unidirectional error (i.e. all bits fail in the same direction) correction/detection are presented for binary block codes. Then ~~we construct~~ are constructed a new class of codes which corrects single errors and detects any number of multiple unidirectional errors. ~~We show here that~~ are shown some codes which hither-to-fore known to possess only symmetric error detection/correction properties which can be modified to make them suitable for unidirectional error correction/detection.



I. INTRODUCTION

Error correcting and/or detecting codes have been extensively discussed for improving the reliability of computer systems and communication networks [1-15]. Most of the theory on random error correcting/detecting codes have been developed under the fault assumption of symmetric errors in the data bits. The predominant faults in some of the recently developed LSI memories are of unidirectional type (i.e. all bits fail in the same direction) rather than symmetric type [15,16]. For example, Cook et. al. [15], have analysed the nature of faults in integrated circuits and come to the following conclusion.

".... any number of bits may fail but they all fail in the same direction, either s-a-1 or s-a-o. Both no access and multiple access of words from a memory cause unidirectional errors. Also, most failures on a chip that affect multiple bits on that chip, e.g., power failures, tend to affect all parallel bits in the same direction ...."

These unidirectional failure properties of some of LSI memories have provided the basis for a new direction of study in coding theory and fault-tolerant computing.

In this report, we develop the basic theory for unidirectional error correction/detection for binary block codes. Some of the background material useful for this report is presented in Section II. In Section III, we establish the necessary and sufficient conditions on binary block codes for unidirectional error correction/detection. In Section IV we construct a new class of codes which is capable of correcting single errors and detecting any number of multiple unidirectional errors. The unidirectional error correcting/detecting capabilities of some of the known codes are discussed in Section V.

II. ASYMMETRIC, UNIDIRECTIONAL AND SYMMETRIC ERRORS AND THE CONCEPT OF ASYMMETRIC DISTANCE*

To use the terminology introduced by Kim and Freiman [18], we will refer to the transition $0 \rightarrow 1$ as 0-error and to the transition $1 \rightarrow 0$ as 1-error. For this report we make a clear distinction among asymmetric, unidirectional and symmetric errors as follows.

Asymmetric errors are those in which all errors in the received words are of only one type (say 1-errors) at all times. This assumption will be appropriate for memories or channels which have asymmetric properties [17-24].

Unidirectional errors are those in which all errors in a received word are of type 0-errors or 1-errors but both the types of errors do not appear simultaneously in any word.

Symmetric errors are those in which both 0-errors and 1-errors can appear simultaneously in a received word.

The following remarks will help clarify further.

If we assume that only asymmetric 1-errors can occur in the code words, then this implies, the probability of occurrence of 0-errors is zero. This type of channel is called ideal binary asymmetric channel by Rao and Chawla [23]. On the other hand, if we assume the errors are of unidirectional nature, then this implies that occurrence of 0-errors and 1-errors is equally likely but the probability of simultaneous occurrence of both 0-errors and 1-errors in the bits of a received word is zero. Finally if we assume the errors are of symmetric type, then the probability of occurrence of 0-errors and 1-errors are equally likely. A channel model that is commonly used for symmetric random errors is the binary symmetric channel [2].

- - - - - - -

*The reader is assumed to be familiar with the basic concepts of coding theory, such as, Hamming distance, minimum distance of a code, minimum distance-error detection/correction relationships.

Let X and Y be two n-tuples over GF(2) = {0,1}. We denote the number of $1 \to 0$ crossovers from X to Y by N(X,Y). Note that in general $N(X,Y) \neq N(Y,X)$.

For example when X = (110110) and Y = (001110) then N(X,Y) = 2 and N(Y,X) = 1.

It is well known that the concept of Hamming distance [1] is useful in discussing the symmetric - error correcting/detecting abilities of codes. This is defined below.

Definition 2.1. The Hamming distance between two n-tuples X and Y, denoted by $D_h(X,Y)$ is defined to be the number of positions in which the two words differ.

In terms of $1 \to 0$ crossover, we can express the Hamming distance between two n-tuples X and Y as

$$D_h(X,Y) = N(X,Y) + N(Y,X) \tag{2-1}$$

Rao and Chawla [23] have defined 'asymmetric distance' with reference to the asymmetric error correcting capability of binary codes as follows:

Definition 2.2. The asymmetric distance between n-tuples X and Y, denoted by $D_a(X,Y)$ is defined to be the maximum number of possible $1 \to 0$ crossovers from X to Y or from Y to X.

$$\text{i.e.} \qquad D_a(X,Y) = \max[N(X,Y),\ N(Y,X)] \tag{2-2}$$

It is shown in [23], that asymmetric distance is a metric, which means D_a satisfies (2-3).

$$\left.\begin{array}{ll} \textcircled{1} & D_a(X,Y) = 0 \text{ iff } X = Y \\ \textcircled{2} & D_a(X,Y) = D_a(Y,X) \\ \textcircled{3} & D_a(X,Z) \leq D_a(X,Y) + D_a(Y,Z) \end{array}\right\} \tag{2-3}$$

The following theorem gives the asymmetric error correcting capability of binary codes.

Theorem (Rao and Chawla [23])

A binary code 'C' of minimum asymmetric distance d_a is capable of correcting d_a-1 or fewer asymmetric 1-errors (or 0-errors).

Outline of the proof:

For any codeword X, let S_x denote the set of vectors obtained from X by replacing 1's with 0's in t places, where $t \leq d_a-1$. Then for any two codewords X and Y, we need to show the corresponding S_x and S_y are disjoint. Since for all $X,Y \in C$, $D_a(X,Y) \geq d_a$ holds, it is straight forward to show S_x and S_y are disjoint. A formal proof can be found in [23].

Remarks

Note that $D_h(X,Y) = d$ implies $D_a(X,Y) \geq \left[\frac{d+1}{2}\right]$, where [r] denotes the integer part of r. We know that a code 'C' with minimum Hamming distance 2t+1 is capable of correcting t or fewer symmetric errors. For this code C, the minimum asymmetric distance will be at least t+1 and hence C is capable of correcting t or less asymmetric errors. Since the condition required for asymmetric error correction is less restrictive than for symmetric error correction, it is expected that for a given n, a t-asymmetric error correcting code to have more codewords (i.e. higher information rate) than a t-symmetric error correcting code. Research in this particular direction has led to the derivation of "Group-Theoretic codes" [24]. The Group-Theoretic codes are single asymmetric-error correcting codes having information rates better than single symmetric error correcting codes such as Hamming codes. Also see the references [18-24].

III. NECESSARY AND SUFFICIENT CONDITIONS FOR UNIDIRECTIONAL ERROR CORRECTION/DETECTION

In this section we establish the necessary and sufficient conditions for unidirectional error detection and correction. The concepts of both Hamming distance and asymmetric distance are useful in establishing these conditions. We start with the following definition.

Definition 3.1. A vector $X = (x_1 \ldots x_n)$ is said to cover vector $Y = (y_1 \ldots y_n)$ if for all i, $y_i = 1$ implies $x_i = 1$. We represent X covers Y by $Y \leq X$. If $X \not\leq Y$ and $Y \not\leq X$, then these vectors are said to be 'unordered'. If $X \leq Y$ or $Y \leq X$ then they are said to be an 'ordered pair'.

For example, when $X_1 = (1011)$ and $Y_1 = (1001)$ then $Y_1 \leq X_1$ i.e. X_1 covers Y_1. On the other hand, the vectors $X_2 = (1010)$ and $Y_2 = (0110)$ are unordered since $X_2 \not\leq Y_2$ and $Y_2 \not\leq X_2$.

Note that when the vectors X and Y are unordered then $N(X,Y) > 0$ and $N(Y,X) > 0$. Also note that if X and Y are an ordered pair then the asymmetric distance and Hamming distance between them are equal i.e. If $X \leq Y$ or $Y \leq X$ then

$$D_h(X,Y) = D_a(X,Y).$$

3.1 UNIDIRECTIONAL ERROR DETECTION

It is known that Berger codes [17] and m-out of n-codes [14,15,19] are capable of detecting multiple unidirectional errors in the code words. For completeness we prove the following theorem which gives the necessary and sufficient conditions for unidirectional error detection.

Theorem 3.1

A code C is capable of detecting multiple unidirectional errors iff every pair of code words is unordered

i.e. for distinct $X,Y \in C$

$$N(X,Y) > 0 \quad \text{and} \quad N(Y,X) > 0 \qquad (3\text{-}1)$$

proof

Since for arbitrary X and Y in C, $N(X,Y) > 0$ and $N(Y,X) > 0$, we have the following form in at least two positions say i and j of X and Y

	i	j
X	.....0.....	1
Y	.....1.....	0

Any vector obtained from X due to 1-errors is distinct from Y in position i, and any vector obtained from X due to 0-errors is distinct from Y in position j.

Conversely, if there exists X and Y in C such that $N(X,Y) > 0$ and $N(Y,X) = 0$, then 1-errors [0-errors] in the positions where X differs from Y can transform X to Y[Y to X]. These errors are not detectable.

3.2 UNIDIRECTIONAL ERROR-CORRECTION

It is well known that a code C is capable of correcting t or less symmetric errors iff the minimum Hamming distance of C is at least $2t+1$ [1]. In the following theorem we establish the necessary and sufficient conditions in the case of unidirectional error correction.

Theorem 3.2

A code C is capable of correcting t or fewer unidirectional errors iff the following condition (3-2) holds.

For all distinct $X,Y \in C$

$$\left.\begin{aligned} &D_a(X,Y) = D_h(X,Y) \geq 2t+1 \quad \text{for } X \text{ and } Y \text{ an ordered pair} \\ &D_a(X,Y) \geq t+1 \quad \text{otherwise} \end{aligned}\right\} \quad (3\text{-}2)$$

Before establishing the validity of Theorem 3.2, first we prove the following lemmas which are useful in proving Theorem 3.2. In the following discussion, S_{z1} refers to the set of all vectors obtained from a word Z due to t or fewer (possibly zero) 1-errors and S_{z0} refers to the set of all vectors obtained from a word Z due to t or fewer (possibly zero) 0-errors. Also S_z refers to the set of all vectors obtained from Z due to t or fewer (possibly zero) unidirectional errors, i.e. $S_z = S_{z0} \cup S_{z1}$.

Lemma 3.3

For an ordered pair X and Y, if $D_a(X,Y) = D_h(X,Y) \geq 2t+1$ then $S_x \cap S_y = \phi$.

Proof:

Let $D_h(X,Y) = m \geq 2t+1$. Now for any $X_e \in S_x$, $D_h(X,X_e) = m_1$, where $m_1 \leq t$. Also for any $Y_e \in S_y$, $D_h(Y_e,Y) = m_2$, where $m_2 \leq t$. From triangular inequality property of Hamming distance, we have $D_h(X,Y_e) + D_h(Y_e,Y) \geq D_h(X,Y)$ i.e. $D_h(X,Y_e) \geq D_h(X,Y) - D_h(Y_e,Y) = m - m_2$. But $m - m_2 \geq t+1$. Hence if $Y_e \in S_y$, then $Y_e \notin S_x$, which implies $S_x \cap S_y = \phi$.

Lemma 3.4

For an unordered pair X and Y if $D_a(X,Y) \geq t+1$ then $S_{x1} \cap S_{y1} = \phi$.

Proof:

From hypothesis $D_a(X,Y) = \text{Max}\big(N(X,Y), N(Y,X)\big) = m$ where $m \geq t+1$. Let us assume $N(Y,X) = m \geq t+1$. For any $X_1 \in S_{x1}$, $N(X,X_1) = m_1$

and $N(X_1,X) = 0$ where $m_1 \leq t$. Also for any $Y_1 \in S_{y1}$, $N(Y,Y_1) = m_2$ and $N(Y_1,Y) = 0$ where $m_2 \leq t$. Hence for any $X_1 \in S_{x1}$, $N(Y,X_1) = m_3$ where $m_3 \geq m \geq t + 1$. So if $X_1 \in S_{x1}$ then $X_1 \notin S_{y1}$ which implies $S_{x1} \cap S_{y1} = \phi$.

Lemma 3.5

For an unordered pair X and Y if $D_a(X,Y) \geq t + 1$ then $S_{x1} \cap S_{y0} = \phi$.

Proof:

Since X and Y are unordered pair, X has value 0 and Y has value 1 in at least one position, say position j. Now any $X_1 \in S_{x1}$ has value 0 and any $Y_0 \in S_{y0}$ has value 1 in position j. Therefore if $X_1 \in S_{x1}$ then $X_1 \notin S_{y0}$ which implies $S_{x1} \cap S_{y0} = \phi$.

Lemma 3.6

For an unordered pair X and Y, if $D_a(X,Y) \geq t + 1$, then $S_{x0} \cap S_{y1} = \phi$.

This can be proved similar to Lemma 3.5.

Lemma 3.7

For an unordered pair X and Y if $D_a(X,Y) \geq t + 1$ then $S_{x0} \cap S_{y0} = \phi$.

This can be proved similar to Lemma 3.4.

Lemma 3.8

For an unordered pair X and Y if $D_a(X,Y) \geq t + 1$ then $S_x \cap S_y = \phi$.

Proof:

$$S_x \cap S_y = (S_{x1} \cup S_{x0}) \cap (S_{y1} \cup S_{y0})$$
$$= (S_{x1} \cap S_{y1}) \cup (S_{x1} \cap S_{y0}) \cup (S_{x0} \cap S_{y1}) \cup (S_{x0} \cap S_{y0})$$

Since X and Y are unordered and $D_a(X,Y) \geq t + 1$ $S_{x1} \cap S_{y1} = \phi$ by Lemma 3.4, $S_{x1} \cap S_{y0} = \phi$ by Lemma 3.5, $S_{x0} \cap S_{y1} = \phi$ by Lemma 3.6 and $S_{x0} \cap S_{y0} = \phi$ by Lemma 3.7. Therefore $S_x \cap S_y = \phi$.

Now we give the complete proof for Theorem 3.2.

Proof for Theorem 3.2:

To establish the sufficient condition, we have to prove for every pair of code words X and Y in C, $S_x \cap S_y = \phi$. Consider some arbitrary code words X and Y. When X and Y are an ordered pair then by hypothesis, $D_a(X,Y) = D_h(X,Y) \geq 2t + 1$. Therefore by Lemma 3.3 $S_x \cap S_y = \phi$. When X and Y are an unordered pair, then by hypothesis $D_a(X,Y) \geq t + 1$. Therefore by Lemma 3.8, again $S_x \cap S_y = \phi$. This completes the proof for the sufficient condition.

Conversely, let there be an ordered pair X and Y in C such that $D_a(X,Y) = D_h(X,Y) = m_1 \leq 2t$. Let us assume $N(X,Y) = m_1$ and $N(Y,X) = 0$. Then 1-errors in some $k (k \leq t)$ positions of X and 0-errors in some $m - k$ $(m - k \leq t)$ positions of Y may result same vector which is ambiguous to decode. Therefore if X and Y are an ordered pair in C, then $D_a(X,Y) \geq 2t + 1$ for t or fewer unidirectional error correction. Again, let there be an unordered pair X and Y in C such that $D_a(X,Y) = m_2 \leq t$. Without any loss of generality we assume $N(X,Y) = m_2$ and $N(Y,X) = m_3$ where $m_3 \leq m_2 \leq t$. Now 1-errors [0-errors] in m_2 positions, where X has 1's and Y has 0's of X[Y] and in m_3 positions where X has 0's and Y has 1's of Y[X] will result the same vector which is again ambiguous to decode. Therefore whenever X and Y in C are unordered, $D_a(X,Y) \geq t + 1$ for t or fewer unidirectional error correction.

Remarks

A t-symmetric error correcting code 'C' has minimum Hamming distance at least $2t + 1$. Hence for any two code words X and Y in C if X and Y are unordered pair then $D_a(X,Y) \geq t + 1$ and if X and Y are ordered pair, then $D_a(X,Y) \geq 2t + 1$. Hence a code C capable of correcting t-symmetric error is also capable of correcting t unidirectional errors. Since the conditions required for t-unidirectional error correction is somewhat less restrictive than that of t-symmetric error correction, we may look for unidirectional error correcting codes which have better information rate than symmetric error correcting codes. However note that there is no difference between single symmetric error and single unidirectional error.

3.3 UNIDIRECTIONAL ERROR CORRECTION AND DETECTION

In the case of symmetric errors, a code C is capable of correcting t-errors and simultaneously detecting $d(d \geq t)$ errors iff the minimum Hamming distance of C is at least $t + d + 1$. A somewhat similar result in the case of unidirectional errors is established in Theorem 3.10. We start with the following lemma which is useful in proving Theorem 3.10.

Lemma 3.9

For a pair of vectors X and Y if $N(X,Y) \geq t + 1$ and $N(Y,X) \geq t + 1$ then

$$S_x \cap Q_y = \phi$$

where S_x is as defined before and Q_y is the set of vectors obtained from Y due to $m(m \geq t + 1)$ unidirectional errors in y.

Proof:

Let $N(X,Y) = \ell$ and $N(Y,X) = k$ where $\ell, k \geq t + 1$. For any $Y_e \in Q_y$ either

$$N(Y,Y_e) \geq t+1 \quad \text{and} \quad N(Y_e,Y) = 0 \tag{3-3}$$

or

$$N(Y,Y_e) = 0 \quad \text{and} \quad N(Y_e,Y) \geq t+1 \tag{3-4}$$

Also for any $X_e \in S_x$ either

$$N(X,X_e) \leq t \quad \text{and} \quad N(X_e,X) = 0 \tag{3-5}$$

or

$$N(X,X_e) = 0 \quad \text{and} \quad N(X_e,X) \leq t \tag{3-6}$$

If the condition (3-3) satisfies for any $Y_e \in Q_y$, then $N(X,Y_e) \geq \ell \geq t+1$ or if the condition (3-4) satisfies for any $Y_e \in Q_y$ then $N(Y_e,X) \geq k \geq t+1$. So in both cases if any $Y_e \in Q_y$ then $Y_e \notin S_x$. Therefore $S_x \cap Q_y = \phi$.

Theorem 3.10

A code C is capable of correcting t or fewer unidirectional errors and detecting multiple (t + 1 or more) unidirectional errors iff the condition (3-7) holds.

$$\left.\begin{array}{ll} \text{i.e. for all } X,Y \in C & N(X,Y) \geq t+1 \\ \text{(and also} & N(Y,X) \geq t+1) \end{array}\right\} \tag{3-7}$$

Proof:

Let Q be the set of all vectors obtained from all code words in C due to $m(m \geq t+1)$ unidirectional errors in the code words.

i.e. $$Q = Q_x \cup Q_y \cup \ldots\ldots\ldots$$
$$= \bigcup_{z \in C} Q_z$$

where Q_z is the set of vectors obtained from a code word Z due to $m(m \geq t+1)$ unidirectional errors in Z. In order to prove the sufficient condition we have to prove, for arbitrary X and Y in C

$$S_x \cap S_y = \phi \tag{3-8}$$

$$S_x \cap Q = \phi \tag{3-9}$$

Since for any $X,Y \in C$, $N(X,Y) \geq t+1$, and $N(Y,X) \geq t+1$, then $D_a(X,Y) \geq t+1$. Therefore by Lemma 3.8 $S_x \cap S_y = \phi$ is true. Now

$$S_x \cap Q = (S_x \cap Q_x) \cup (S_x \cap Q_y) \cup \ldots\ldots = \bigcup_{z \in C} S_x \cap Q_z \tag{3-10}$$

$S_x \cap Q_x = \phi$ is true because for any $X_e \in S_x$, $D_a(X,X_e) \leq t$ and for any $X_e' \in Q_x$, $D_a(X,X_e') \geq t+1$. Also for any $Y(\neq X)$ in C, since $N(X,Y) \geq t+1$ and $N(Y,X) \geq t+1$, $S_x \cap Q_y = \phi$ is true by Lemma 3.9. Therefore $S_x \cap Q = \phi$ is true.

Conversely, let there be X and Y in C such that $N(X,Y) = m_1 \leq t$ and $N(Y,X) = m_2$. Let X'[Y'] be the vector obtained from X[Y] by $1 \rightarrow 0$ [$0 \rightarrow 1$] crossovers in m_1 ($m_1 \leq t$) positions where X has 1's and Y has 0's. The same vector X'[Y'] can be obtained from Y[X] by $1 \rightarrow 0$ [$0 \rightarrow 1$] crossovers in the positions where Y has 1's and X has 0's. Hence both X' and Y' are ambiguous to decode. Therefore for any X and Y in C, $N(X,Y) \geq t+1$ and $N(Y,X) \geq t+1$ for t unidirectional error correction and multiple (t + 1 or more) unidirectional error detection.

A stronger result for the code C with the property (3-7) is given in Theorem 3.11. A complete proof is given in the Appendix A.

Theorem 3.11

For all $X,Y \in C$ if $N(X,Y) \geq t+1$ and $N(Y,X) \geq t+1$ then C is capable of correcting t-symmetric errors, detecting t + 1 symmetric errors and also detecting multiple (t + 2 or more) unidirectional errors.

IV. SINGLE ERROR CORRECTING AND MULTIPLE UNIDIRECTIONAL ERROR DETECTING (SEC-MUED) CODES

In this section, we construct a new class of codes which is capable of correcting single errors and detecting multiple (more than one) unidirectional errors. We call these codes as Group Theoretic Single Error Correcting and Multiple Unidirectional Error Detecting (SEC-MUED) codes. In the following discussion we denote the set of code words by 'C', the length of code words by n and the number of code words by M. We start with the following lemma.

Lemma 4.1

A constant weight code 'C' with minimum Hamming distance 4 is capable of correcting single error and detecting multiple unidirectional errors.

Proof:

Since C is a constant weight code, for any $u,v \in C$, $N(u,v) = N(v,u)$. Furthermore, $D_h(u,v) = N(u,v) + N(v,u) = 2N(u,v) \geq 4$. Therefore $N(u,v) \geq 2$. Hence by Theorem 3.10, C is a SEC-MUED code.

A generalization of Lemma 4.1 is as follows.

Lemma 4.2

A constant weight code 'C' with minimum Hamming distance $2t+2$ is capable of correcting t- unidirectional errors and detecting multiple (more than t) unidirectional errors.

This can be proved similar to Lemma 4.1 and hence a formal proof is not given.

From Lemma 4.1, one can see that constant weight code with minimum Hamming distance 4 is a SEC-MUED code. One of the aspects of coding theory problems is to get high information rate codes i.e. for a given n, to come up with maximum number of code words. At this point we can ask the question, "What would be the information rates of SEC-MUED codes if the codes are

generated by applying Lemma 4.1?" Best et. al. [25] have given bounds for the maximum number of code words M_{max}, for constant weight codes with minimum Hamming distance d_h and length n for the range $d_h \leq 10$ and $n \leq 24$. M_{max} for the case $d_h = 4$ is of interest to us and is given in Table I. Note that [n/2] out of n codes have highest information rate. Also note that the information rate of these codes are comparable to Hamming distance 4 SEC-DED codes. (For a given 'n' the redundant bits required for SEC-MUED codes may be at most one greater than that of SEC-DED codes. But at the same time one should note that SEC-MUED codes detect multiple unidirectional errors.) These observations suggest the existence of good information rate SEC-MUED codes and also motivate us to pursue further research in this direction.

Now consider the (7,3) cyclic code 'C' generated by the polynomial $g(x) = x^4 + x^3 + x^2 + 1$. There are eight code words and they are given below:

(000 0000, 001 0111, 010 1110, 011 1001,
100 1011, 101 1100, 110 0101, 111 0010).

Note that between any two nonzero code words u and v in C, $N(u,v) = 2$. Hence the set of nonzero code words of (7,3) cyclic code constitutes a SEC-MUED code with $n = 7$ and $M = 7$. Also if we omit the code words (0000 0000) and (1111 1111) from (8,4) SEC-DED code, the set of remaining code words forms a SEC-MUED code. Hence we have a SEC-MUED code with $n = 8$ and $M = 14$.

In the following paragraphs we give a systematic way of constructing SEC-MUED codes for any n. These are subcodes of Group-theoretic codes developed by Rao and Constantin [24].

n \ k	2	3	4	5	6	7	8	9	10	11	12
4	2	1	1								
5	2	2	1	1							
6	3	4	3	1	1						
7	3	7	7	3	1	1					
8	4	8	14	8	4	1	1				
9	4	12	18	18	12	4	1	1			
10	5	13	30	36	30	13	5	1	1		
11	5	17	35	66	66	35	17	5	1	1	
12	6	20	51	73-84	132	73-84	51	20	6	1	1
13	6	26	65	99--132	143--182	143--182	99-132-	65	26	6	1
14	7	28	91	143--182	210--308	232--364	210--308	143--182	91	28	7
15	7	35	105	213--271	321-455	435--660	435--660	321--455	213--271	105	35
16	8	37	140	305-336-	513--722	?-1040	870--1320	?-1040	513--722	305--336	140
17	8	44	154--157	424--476	792--952	?-1753	?-2210	?-2210	?-1753	792--952	424--476
18	9	48	198	480--565	1188--1428	?-2448	?-3944	?-4420	?-3944	?-2448	1188--1428
19	9	57	228	612--752	1428--1789	?-3876	?-5814	?-8326	?-8326	?-5814	?-3876
20	10	60	285	816--912	2040--2506	?-5111	?-9690	?-12920	?-16652	?-12920	?-9690
21	10	70	315	1071--1197	2856--3192	?-7518	?-13416	?-22610	?-27132	?-27132	?-22610
22	11	73	385	1386	3927--4389	?-10032	?-20674	?-32794	?-49742	?-54264	?-49742
23	11	83	416--419	1771	5313	?-14421	?-28842	?-52833	?-75426	?-104006	?-104006
24	12	88	498	1859--2011	7084	?-18216	?-43263	?-76912	?-126799	?-164565	?-208012

TABLE I. The number of code words M for constant weight code with Hamming distance 4 (Table from ref. [25])
n = length, k = Hamming weight

Let G be an additive Abelian group of order $n + 1$ having elements $(a_0, a_1, a_2 \ldots\ldots a_n)$ where a_0 is the identity element. Let $B = \{0,1\}$. Consider the set V, where $V = \{v/v \in B^n\}$. Note that $|V| = 2^n$.

We define a function $T: V \to G$ such that

$$T(v) = T((\alpha_1, \alpha_2 \ldots\ldots \alpha_n)) = \sum_{i=1}^{n} \alpha_i a_i \qquad (4\text{-}1)$$

where

$$\alpha_i a_i = \begin{cases} a_0 & \text{for } \alpha_i = 0 \\ a_i & \text{for } \alpha_i = 1 \end{cases} \qquad (4\text{-}2)$$

The operation of summation in the equation (4-1) is group operation.

Now consider the set V', where $V' = \{u | u \in B^n$ and u has $k (k \geq 2)$ 1's and n-k 0's$\}$. Note that $V' \subset V$ and $|V'| = \binom{n}{k} = \frac{n!}{n!n-k!}$.

The function T defined above, will partition the set V' of $\binom{n}{k}$ elements into (n+1) mutually disjoint sets. i.e.

$$\left.\begin{aligned} V' &= V_0 \cup V_1 \cup \ldots\ldots \cup V_n \\ V_i \cap V_j &= \phi \qquad\qquad i,j = 0,1,2,\ldots.n \quad i \neq j \end{aligned}\right\} \qquad (4\text{-}3)$$

where the set V_i is defined as follows.

$$V_i = \left\{ v = (\alpha_1 \alpha_2 \ldots \alpha_n) \in V' \Big| \sum_{j=1}^{n} \alpha_j a_j = a_i \right\} \qquad (4\text{-}4)$$

The following example illustrates the construction of such a set using the additive group of $GF(2^3)$.

Example 4.1 The additive table for the additive group of $GF(2^3)$ is given below.

	a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7
	0	1	X	X^2	1+X	$1+X^2$	$1+X+X^2$	$X+X^2$
0	0	1	X	X^2	1+X	$1+X^2$	$1+X+X^2$	$X+X^2$
1	1	1	1+X	$1+X^2$	X	X^2	$X+X^2$	$1+X+X^2$
X	X	1+X	0	$X+X^2$	1	$1+X+X^2$	$1+X^2$	X^2
X^2	X^2	$1+X^2$	$X+X^2$	0	$1+X+X^2$	1	1+X	X
1+X	1+X	X	1	$1+X+X^2$	0	$X+X^2$	X^2	$1+X^2$
$1+X^2$	$1+X^2$	X^2	$1+X+X^2$	1	$X+X^2$	0	X	1+X
$1+X+X^2$	$1+X+X^2$	$X+X^2$	$1+X^2$	1+X	X^2	X	0	1
$X+X^2$	$X+X^2$	$1+X+X^2$	X^2	X	$1+X^2$	1+X	1	0

The vectors in the set V_0 are

$$v_1 = (1110010)$$
$$v_2 = (1100101)$$
$$v_3 = (1011001)$$
$$v_4 = (1001110)$$
$$v_5 = (0111100)$$
$$v_6 = (0101011)$$
$$v_7 = (0010111)$$

Every vector $v_i = (\alpha_1\alpha_2\alpha_3\alpha_4\alpha_5\alpha_6\alpha_7) \in V_0$, has the property

$$\sum_{i=1}^{T} \alpha_i a_i = a_0 .$$

The other sets V_1, V_2 .... V_7 can be constructed similarly.

The following lemma is a direct consequence of property (4-3).

Lemma 4.1

At least one of the sets V_0, V_1 .... V_n has cardinality greater than or equal to $\frac{\binom{n}{k}}{n+1}$

i.e. $|V_i| \geq \frac{\binom{n}{k}}{n+1}$ for some $i = 0, 1, \ldots n.$ (4-5)

Remark:

If $\binom{n}{k}$ is not divisible by n+1 then (4-5) holds with strict inequality.

Next, we will consider one of the partitions V_i, induced by G in the set of vectors V and establish the following important result in constructing SEC-MUED code.

Theorem 4.2

For any two arbitrary vectors u and v of V_i, the minimum number of $1 \rightarrow 0$ cross-overs from u to v is at least 2.

i.e. $N(u,v) \geq 2$ for all $u,v \in V_i$.

Proof:

Suppose there exists two vectors u and v in V_i such that N(u,v) is just 1. Since the Hamming weight of each code word is same, the following case is the only alternative.

$$\begin{aligned} u &= (\alpha_1\alpha_2 \ldots\ldots \alpha_{k-1}\ 1\ \alpha_{k+2} \ldots\ldots \alpha_{\ell-1}\ 0\ \alpha_{\ell+1} \ldots\ldots \alpha_n) \\ v &= (\alpha_1\alpha_2 \ldots\ldots \alpha_{k-1}\ 0\ \alpha_{k+2} \ldots\ldots \alpha_{\ell-1}\ 1\ \alpha_{\ell+1} \ldots\ldots \alpha_n) \end{aligned} \tag{4-6}$$

where $k \neq \ell$.

Since $u,v \in V_i$

$$\sum_{\substack{j=1 \\ j\neq k \\ j\neq \ell}}^{n} \alpha_j a_j + a_k = \sum_{\substack{j=1 \\ j\neq k \\ j\neq \ell}}^{n} \alpha_j a_j + a_\ell = a_i \tag{4-7}$$

Hence we get

$$a_k = a_\ell = a_i - \sum_{\substack{j=1 \\ j\neq k \\ j\neq \ell}}^{n} \alpha_i a_j \tag{4-8}$$

This gives the contradiction because $a_k \neq a_\ell$ for $k \neq \ell$. Hence for distinct $u,v \in V_i$, $N(u,v) \geq 2$.

By consequence of Theorems 3-10 and 4-2, one can see that the sets of vectors V_0, V_1, ... V_n individually can be used as SEC-MUED codes.

We explain below how error correction/detection process can be implemented for the above SEC-MUED code. An ordering of the elements of the group G is presupposed for purposes of uniquely determining the faulty position.

Let the set of vectors V_i constitute SEC-MUED code. Let us assume that the number of 1's in each code word is k where $k \geq 2$. If an error say 0-error occurs in a code word $v \in V_i$ resulting the word $v' = (\alpha_1 \alpha_2 \ldots \alpha_n)$ such that

$$\sum_{j=1}^{n} \alpha_j a_j = a_\ell,$$

then the number of 1's in the word v' will be k+1 and hence it is immediately known the existence of a 0-error in the word v'. The position r in error can be located by

$$a_r = a_\ell - a_i.$$

Thus r is determined, and therefore correction can be implemented.

On the other hand, if an 1-error occurs in a code word $u \in V_i$, resulting a word $u' = (\beta_1 \beta_2 \ldots \beta_n)$ such that

$$\sum_{j=1}^{n} \beta_j a_j = a_m,$$

then the number of 1's in the word u' will be k-1 and it is immediately known the existence of a 1-error in u'. The position s in error can be located by $a_s = a_i - a_m$. Once s is obtained, error correction can be implemented.

Finally, if more than one 0-error occurs in any code word $w \in V_i$, then the number of 1's in the received word w' will be greater than k+1 and if more than one 1-error occurs in any code word $w \in V_i$, then the number of 1's in the received word will be less than k-1. In both cases the multiple unidirectional errors can be detected.

The following example illustrates the above concept.

Example 4.2 Consider the additive group Z_9 whose group operation is mod 9 addition. The code words in the set V_0 are

$$\begin{array}{r} 8\ 7\ 6\ 5\ 4\ 3\ 2\ 1 \\ v_1 = (1\ 1\ 0\ 0\ 0\ 0\ 1\ 1) \\ v_2 = (1\ 0\ 1\ 0\ 0\ 1\ 0\ 1) \\ v_3 = (1\ 0\ 0\ 1\ 1\ 0\ 0\ 1) \\ v_4 = (1\ 0\ 0\ 1\ 0\ 1\ 1\ 0) \\ v_5 = (0\ 1\ 1\ 0\ 1\ 0\ 0\ 1) \\ v_6 = (0\ 1\ 1\ 0\ 0\ 1\ 1\ 0) \\ v_7 = (0\ 1\ 0\ 1\ 1\ 0\ 1\ 0) \\ v_8 = (0\ 0\ 1\ 1\ 1\ 1\ 0\ 0) \end{array}$$

Suppose an erroneous message $v' = (1000\ 0011)$ is received, the existence of 1-error in the word is readily evident because the weight of v' is only 3. Also $T(v') = 8 + 2 + 1 = 2$ and since $0 - 2 = -2 = 7$, the seventh bit of v' is in error. Hence the actual message transmitted is the code word $v' = (1100\ 0011)$.

On the other hand, if the erroneous received message is $u' = (1101\ 0011)$, again the existence of a 0-error is readily evident because the weight of u' is 5. Since $T(u') = 8 + 7 + 5 + 2 + 1 = 5 = 0 + 5$, the fifth bit of u' is in error. The actual transmitted message is again the code word $v_1 = (1100\ 0011)$.

Computation of the Number of Redundant Bits in a SEC-MUED Code

One of the aspects of coding theory is to obtain codes with as high information rate as possible. That is, we wish to have the cardinality of the code approach the theoretical maximum which we denoted by M_{max}. For the group-theoretic SEC-MUED codes, at present time, we don't have a closed formula to find out M_{max}. For a particular group G_1 of order $n+1$, to find out M_{max}

in a Group theoretic SEC-MUED code, two important points need further investigation.

1. What should be the optimal value of k, the number of 1's in a code word, and
2. Which subset V_i has the highest cardinality.

From Table I we can see that M will be maximum when $k = \left[\frac{n}{2}\right]$ where [r] is the integer part of r. Hence we conjecture that M will be maximum when $k = \left[\frac{n}{2}\right]$. The second question is under investigation.

In the following lemma we calculate the upper bound for the number of redundant bits required in the Group theoretic SEC-MUED code.

Lemma 4.3

For large values of n, the number of redundant bits required for the Group theoretic SEC-MUED code is less than or equal to $\left[\frac{3}{2}\log_2(n+1)\right] + 1$.

Proof:

By Lemma 4.1 $$M \geq \frac{\binom{n}{k}}{n+1}$$ where

M is the number of code words, n is the length and k is the number of 1's in each code word

when $$k = \left[\frac{n}{2}\right]$$

$$\binom{n}{k} = \frac{n!}{\left[\frac{n}{2}\right]!\left(n - \left[\frac{n}{2}\right]\right)!}$$

$$\approx \frac{n!}{\left(\left[\frac{n}{2}\right]!\right)^2}$$

Using Stirling approximation for factorial function (i.e. $n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)$ for large n) we have

$$\frac{n!}{\left(\left[\frac{n}{2}\right]!\right)^2} \simeq \frac{\sqrt{2\pi n}\left(\frac{n}{e}\right)^n}{\left(\sqrt{2\pi n/2}\left(\frac{n}{2e}\right)^{\frac{n}{2}}\right)^2}$$

$$\simeq \frac{2^n}{\sqrt{n}}$$

Therefore

$$M \geq \frac{2^n}{\sqrt{n}\ (n+1)} \geq \frac{2^n}{(n+1)^{3/2}}$$

i.e. $$\log M \geq n - \frac{3}{2} \log (n+1)$$

$$n - \log M \leq \frac{3}{2} \log (n+1)$$

Hence the lemma is proved.

V. OTHER UNIDIRECTIONAL ERROR DETECTING AND CORRECTING CODES

In this section we discuss the unidirectional error correcting/detecting properties of some existing codes which were developed for symmetric error correction/detecting. We will study mainly the unidirectional error correcting/detecting properties of equidistance linear codes and the codes generated from Hadamard matrices [2,3].

a. Equidistance linear codes

Definition 5.1 A code C is called equidistance code iff the Hamming distance between every pair of code words is the same.

The dual code of single error correcting Hamming code is an example of equidistance code. So, for any m ($m > 0$) we can have $(2^m - 1, m)$ equidistance linear code [2,3]. The Hamming distance between every pair of code words in a equidistance code is 2^{m-1} and the Hamming weight of each nonzero code word is also 2^{m-1}.

Example 5.1

A (15,4) equidistance linear code can be represented by the generated matrix

$$\begin{pmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{pmatrix}$$

Note that the generated matrix G for (15,4) equidistance code is also the parity matrix of (15,11) Hamming single error correcting code. The Hamming distance between every pair of code words in the code generated by G is exactly 8.

Next, we discuss the unidirectional error-correcting/detecting properties of these codes.

Lemma 5.1

If C is a $(2^m - 1, m)$ equidistance linear code, then for every pair of nonzero code words $u,v \in C$, we have $N(v,u) = N(u,v) = 2^{m-2}$.

Proof

Since the Hamming weight of nonzero code words is constant (i.e. 2^{m-1}) for all nonzero $u,v \in C$, $N(u,v) = N(v,u)$. Furthermore for all nonzero $u,v \in C$, $D_h(u,v) = N(u,v) + N(v,u) = 2N(u,v) = 2^{m-1}$. Therefore for all nonzero $u,v \in C$, we have $N(u,v) = N(v,u) = 2^{m-2}$.

By consequence of Theorem 3.10 and Lemma 5.1, one can easily verify that by simply omitting the $\underline{0}$ vector from $(2^{m-1}, m)$ linear equidistance code, the set of remaining code words C_1 is capable of correcting $2^{m-2} - 1$ unidirectional errors and detecting any number of unidirectional errors. The number of code words M, in C, will be $2^m - 1$. Note that when C is used for symmetric error correction/detection, it is capable of correcting $2^{m-2} - 1$ symmetric errors and detecting 2^{m-2} symmetric errors.

For example (15,4) equidistance code is capable of correcting 3 symmetric errors and detecting 4 symmetric errors. If we omit the $\underline{0}$ code word from the code, the set of remaining code words is capable of correcting 3-unidirectional errors and detecting any number of multiple unidirectional errors.

Consider the first order Reed-Muller code C [2,3] which is of the form $(2^m, m+1)$. If we omit the $\underline{0}$ code word and all one code word from C, the set of remaining code words C' has the following property. i.e. for all $u,v \in C'$, $N(u,v) = 2^{m-2}$. Therefore C' is also capable of correcting $2^{m-2} - 1$ unidirectional errors and detecting multiple unidirectional errors with $n = 2^m$ and $M = 2^{m+1} - 2$.

b. Codes generated from Hadamard Matrices

The codes generated from this method are also equidistance codes but not necessarily linear codes.

Definition 5.2

A Hadamard matrix of order n is an $n \times n$ matrix H with +1's and -1's as entries and is such that

$$H H^T = n I, \tag{5-1}$$

where nI is the diagonal matrix with n's in the diagonal.
In other words, the inner product of any two distinct rows is equal to 0, whereas the inner product of a row with itself is equal to n.

Definition 5.3

A Hadamard matrix is said to be normalized if its first row and first column consist entirely of +1's.

Example 5.2

A normalized Hadamard matrix of order 8×8 is given below.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \end{pmatrix}$$

It is shown in [2,3], that if there exists an $n \times n$ Hadamard matrix, there exists a binary code with n symbols, $2n$ code words and minimum Hamming distance $n/2$. The following theorem gives the unidirectional error correcting/detecting properties of the codes generated by Hadamard matrices.

Theorem 5.2

If there exists an $n \times n$ Hadamard matrix ($n \geq 4$), there exists a code 'C' with n symbols, $2n-2$ code words and $N(u,v) \geq \frac{n}{4}$ for arbitrary distinct u,v in C.

Proof

Let H be an $n \times n$ normalized Hadamard matrix. The code C is constructed as follows. Form a set of $2n$ vectors C', from $v_1, v_2 \ldots . v_n, -v_1, -v_2 \ldots . -v_n$ where $v_1, v_2 \ldots . v_n$ are the rows of H. Let v_1 be the all +1 vector. Then in each of C' change +1 to 1 and -1 to 0. Omit the all 1 vector and the zero vector. The set of remaining vectors constitutes the code C with $|C| = 2n-2$. Next we prove for distinct $u,v \in C$

$$N(u,v) = \frac{n}{4} \quad \text{for} \quad v \neq \bar{u}$$

$$= \frac{n}{2} \quad \text{for} \quad v = \bar{u}. \qquad (5\text{-}2)$$

Since each of vectors C' is orthogonal to v_1, the number of 1's in each of the code word is $n/2$. Hence it is straight forward to prove $N(u,v) = n/2$ for $v = \bar{u}$. Also since $\pm v_j$ is orthogonal to $\pm v_i$ if $i \neq j$, they must match in half the positions and differ in the other half positions and thus the corresponding code words are at a Hamming distance $n/2$. Therefore $N(u,v) = \frac{n}{4}$ for $v \neq \bar{u}$ can be proved similar to Lemma 5.1. This completes the proof.

Hence, the code C' generated from an $n \times n$ Hadamard matrix [2,3] is capable of correcting $(\frac{n}{4}-1)$ symmetric errors and detecting $\frac{n}{4}$ symmetric errors. On the other hand if we omit the zero vector and all one vector, the set of resultant code words C, is capable of correcting $(\frac{n}{4}-1)$ unidirectional errors and detecting multiple unidirectional errors. If H is an Hadamard matrix of order n, then it can be proved that n is a multiple of 4 [26].

The following theorem gives how to construct higher order Hadamard matrices from known lower order Hadamard matrices.

Theorem 5.3

If H is an $n \times n$ Hadamard matrix then the matrix

$$H' = \begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

is also a $2n \times 2n$ Hadamard matrix.

It is straight forward to prove $H' H'^{T} = 2nI$ and hence the proof is omitted.

Other methods of constructing Hadamard matrices can be found in [26]. Hadamard matrices of any order which is less than 200 and multiple of 4 except 188 are known. Higher order Hadamard matrices can be constructed by using Theorem 5.3.

VI. CONCLUSION

In this report the necessary and sufficient conditions required for binary block codes to correct/detect unidirectional errors have been established. A new class of codes which corrects single errors and detects multiple unidirectional errors is also presented. We have established here that the equidistance linear codes, first order Reed-Muller codes and the codes generated from Hadamard matrices, which are known to have symmetric error correcting/detecting properties, can be modified to make them suitable for unidirectional error correction/ detection.

In this report we have not considered the encoding/decoding problems. Use of ROMS for encoding/decoding of SEC-MUED codes looks to be a feasible solution. These problems along with construction of separable SEC-MUED codes are under investigation.

APPENDIX A

PROOF FOR THEOREM 3.11

Before establishing the Theorem 3.11, we prove the following lemma which is useful in proving Theorem 3.11. In the following discussion T_z refers to the set of vectors obtained from Z due to m_1 ($0 \leq m_1 \leq t$) symmetric errors in Z and Q_z' refers to the set of vectors obtained from Z due to m_2 ($m_2 \geq t + 2$) unidirectional errors in Z.

Lemma A.1

For a pair of vectors X and Y, if $N(X,Y) \geq t + 1$ and $N(Y,X) \geq t + 1$ then

$$T_x \cap Q_x' = \phi \qquad \text{(A-1)}$$

and

$$T_x \cap Q_y' = \phi \qquad \text{(A-2)}$$

Proof:

For all $X' \in T_x$, $D_h(X, X') \leq t$. For any $Y' \in Q_y'$, if Y' is obtained from Y due to m ($m \geq t + 2$) 1-errors [or 0-errors], then $N(X,Y') \geq t + 1$ [or $N(Y',X) \geq t + 1$]. In both cases $D_h(X,Y') \geq t + 1$. Therefore if $Y' \in Q_y'$ then $Y' \notin T_x$ which implies $T_x \cap Q_y' = \phi$. Equation (A-1) is obvious by definitions of T_x and Q_x'.

Proof for Theorem 3.11

The minimum Hamming distance of C is at least $2t + 2$, because for all $X,Y \in C$, $D_h(X,Y) = N(X,Y) + N(Y,X) \geq 2t + 2$. Hence C is t symmetric error correcting and $t+1$ symmetric error detecting code. Hence it is sufficient to prove that C is capable of simultaneously detecting multiple ($t + 2$ or more) unidirectional errors. Let Q' be the set of vectors obtained from all code words in C due to $t + 2$ or more unidirectional errors.

i.e. $$Q' = Q_x' \cup Q_y' \cup \ldots.$$

$$= \bigcup_{z \in C} Q_z$$

So we have to prove for arbitary $X \in C$, $T_x \cap Q' = \phi$. But $T_x \cap Q' = (T_x \cap Q_x') \cup (T_x \cap Q_y') \cup \ldots..$ By Lemma A.1, each term of the form $T_x \cap Q_z'$ is empty and therefore their union $T_x \cap Q' = \phi$. That completes the proof.

REFERENCES

1. R.W. Hamming, "Error Detecting and Error Correcting Codes," Bell System Technical Journal, Vol. 29, pp. 147-160, April 1950.

2. W.W. Peterson, E.J. Weldon, "Error Correcting Codes," MIT Press, Cambridge, Massachusetts, 1972.

3. E.R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill, 1968.

4. E.R. Berlekamp, "Key Papers in the Development of Coding Theory," IREE Press, 1974.

5. S. Lin, "An Introduction to Error-Correcting Codes," Prentice Hall, Inc., 1970.

6. F.F. Sellers, M.Y. Hsiao and L.W. Bearnson, "Error Detecting Logic for Digital Computers," McGraw-Hill, New York.

7. T.R.N. Rao, "Error Coding for Arithmetic Processors," Academic Press, New York.

8. J.F. Wakerly, "Error Detecting Codes, Self-checking Circuits and Applications," North Holland, New York, 1978.

9. M.Y. Hsiao, " A Class of Optimal Minimum Odd-Weight Column SEC-DED Codes," IBM J. Res. Develop., pp. 395-401, July 1970.

10. D.C. Bossen, "b-Adjacent Error Correction," IBM J. Res. Develop., pp. 402-408, July 1970.

11. S.J. Hong and A.M. Patel, "A General Class of Maximal Codes for Computer Applications," IEEE Trans. on Computers, Vol. C-21, pp. 1322-1331, Dec. 1972.

12. W.C. Carter and C.E. McCarthy, "Implementation of an Experimental Fault-Tolerant Memory System," IEEE Trans. Comput., Vol. C-25, pp. 557-568, June 1976.

13. L. Levine and W. Meyers, "Semiconductor Memory Reliability with Error Detecting and Correcting Codes," Computer, pp. 43-50, Oct. 1976.

14. D.A. Anderson and G. Metze, "Design of Totally Self-Checking Check Circuits for m-out-of-n Codes," IEEE Trans. on Computers, Vol. C-22, pp. 263-269, March 1973.

15. R.W. Cook, W.H. Sisson, T.F. Storey and W.N. Toy, "Design of a Self-Checking Microprogram Control," IEEE Trans. on Computers, Vol. C-22, pp. 255-262, March 1973.

16. R.W. Sahni, "Reliability of Integration Circuits," Proc. of IEEE Inter. Computer Group Conf., pp. 213-319, Washington, D.C., June 1970.

17. J.M. Berger, "A Note on Error Detecting Codes for Asymmetric Channels," Information and Control, Vol. 4, pp. 68-73, March 1961.

18. W.H. Kim, C.V. Freiman, "Single Error Correcting Codes for Asymmetric Channels," IRE Transactions on Information Theory, pp. 62-66, June 1959.

19. C.V. Freiman, "Optimal Error Detection Codes for Completely Asymmetric Binary Channels," Information and Control, Vol. 5, pp. 64-71, 1962.

20. R.R. Varshamov, "Some Features of Linear Codes that Correct Asymmetric Errors," Cybernetics and Control Theory, Vol. 9, No. 7, pp. 538-540, Jan. 1965. (Translated from Doklady Akademii Nauk SSSR, Vol. 157, No. 3. pp. 546-548, July 1964.)

21. R.R. Varshamov, "On the Theory of Asymmetric Codes," Cybernetics and Control Theory, Vol. 10, No. 10, pp. 901-903, April 1966. (Translated from Doklady Akademii Nauk SSSR, Vol. 164, No. 4, pp. 757-760, Oct. 1965.)

22. R.R. Varshamov, "A Class of Codes for Asymmetric Channels and a Problem from Additive Theory of Numbers," IEEE Trans. Inf. Theory, Vol. IT-19, No. 1, pp. 92-95, Jan. 1973.

23. T.R.N. Rao and A.S. Chawa, "Asymmetric Error Codes for Some LSI Semi-Conductor Memories," The Annual Southeastern Symposium on System Theory, pp. 170-171, March 1975.

24. T.R.N. Rao and Constantin, "Group Theoretic Codes for Binary Asymmetric Channels," Technical Report CS 76014, Dept. of Computer Science, Southern Methodist University, October 1976.

25. M.R. Best, A.E. Brouwer, F.J. MacWilliams, A.M. Odlyzko, N.J.A. Sloane, "Bounds for Binary Codes of Length Less than 25," IEEE Trans. Inf. Theory, Vol. IT-24, No. 1, pp. 81-93, Jan. 1978.

26. Marshall Hall, Jr., "Combinatorial Theory," Blaisdell Publishing Co., Watham, Massachusetts, 1967.