CHAPTER-3

UPPER BOUND ON CORRECTING PARTIAL RANDOM ERRORS

The contents of this Chapter are based on my following published paper:

CHAPTER-3

UPPER BOUND ON CORRECTING PARTIAL RANDOM ERRORS

3.1 INTRODUCTION

Since coding has become a basic tool for practically all communication/electronic devices, it is important to study the error patterns that actually occur. This allows correction of only partial errors in \( (n,k) \) codes over \( \mathbb{Z}_q \), \( q > 3 \) rather than those which have been studied using Hamming distance, in non-binary cases.

The chapter considers a class of distances, SK-distances, in terms of which partial errors can be defined. We examine the sufficient condition for the existence of parity check matrix for a given number of parity-checks; the chapter contains an upper bound on number of parity check digits for linear codes with the property that they correct all partial random error of an \( (n,k) \) code with minimum SK-distance at least \( d \). The result is a generalization of the rather widely used Varshamov-Gilbert bound which is given in Chapter-1, recalling the statement of this bound, it states:

A sufficient condition for existence of an \( (n,k) \) code over \( GF(q) \) with minimum Hamming distance at least \( d \) is that \( n,k,q \) and \( d \) are such that they satisfy the inequality

\[
\sum_{i=0}^{d-2} \binom{n}{i} (q-1)^i < q^{n-k} \text{ [78].}
\]

It will be found that bound follows from our result as a particular case.

Before moving further here we bear in mind the idea of partial error pattern and Limited Error pattern which we defined in earlier Chapter-2 as follows:
PARTIAL ERROR PATTERN AND PATTERNS OF LIMITED ERROR

PARTIAL SETS

Recall that in defining the SK-partition $\mathcal{Q} = \{B_0, B_1, \ldots, B_{m-1}\}$ of $\mathbb{Z}_q$, $B_i$'s arranged in a circular order, $B_s$ is in fact the collection of all elements of $\mathbb{Z}_q$ at distance $s$, on either side of 0, each element of which is assigned an SK weight $s$. We can thus call $B_s$ subset or ‘partial set’ of $\mathbb{Z}_q$, of weight $s$ and at distance $s$ from 0.

More generally, for an arbitrary element $j \in \mathbb{Z}_q$ its ‘partial set at distance $s$’ is given by $B_s(j) = \{B_s + j\}_q$, the addition being in each element of $B_s \mod q$.

PATTERNS OF LIMITED ERRORS

We know that error detection/correction studies are made taking into consideration the patterns of errors, which vary from system to system. Study of block/linear codes is also limited to errors in which an entry in a code word is received as another symbol, the error is called a ‘substitution error’. With SK-scheme of things, it is possible to consider various different limited kinds of substitution errors that were not possible under Hamming scheme of things. These can be in terms of:

(i) The number of places of the errors (random or bursts),
(ii) Substitutions limited to one or more of $B_i$’s,
(iii) Maximum overall SK-weight of the error patterns,
(iv) Combinations of any two or three of the above.

In obtaining a bound on necessary number of parity-checks for an $e$-error correcting code, it is customary to define volume of a sphere of radius $e$ around every code word and consider their mutual disjoint-ness etc. In the SK-study that we undertake, this idea can be looked upon more closely. Given an $n$-vector $u$, we can find numbers of patterns which have specified SK-distance from vector $u$. 
We will need a generalization, which we call, ‘partial independence’, of vectors.

PARTIAL INDEPENDENCE

DEFINITION: $B$-INDEPENDENCE

Given a set of $n$-vectors $S$ over the field $GF(q)$, and a subset $B$ of $GF(q)$, the set of vectors $S$ will be called partially independent in $B$, if all linear combination of vectors in $S$, with coefficients from $B$, some non-zero, is not zero. In this situation $S$ may be termed ‘$B$-independent’.

In previous Chapter-1, we obtained a necessary condition giving number of parity check digits for linear codes correcting SK-distance limited partial random error on $e$ or fewer positions.

3.3 SUFFICIENT CONDITION ON NUMBER OF PARITY CHECK DIGITS

This section presents sufficient condition on number of parity check digits for linear codes with property that correct all random error of an $(n,k)$ code with minimum distance at least $d$, with entries limited to $B_1$, as also $B_1$ or $B_2$.

THEOREM 3.1: Given an SK-partition $\varnothing = \{B_0, B_1, \ldots, B_{m-1}\}$ of $Z_q$, $q$ prime, a sufficient condition for the existence of an $(n,k)$ code over $Z_q$, with minimum SK-distance at least $d$, when entries in a position of any two code words differ only partially by entry from $B_1$, is given by

$$\sum_{i=0}^{d-2} \binom{n}{i} |B_i|^i \geq q^{n-k}.$$  

PROOF: Obviously, the existence of such an $(n,k)$ code is ensured by constructing a parity check matrix $H$, with $n$ columns and $r = n - k$ rows. Here condition for its existence is to be examined to suite the code in question. We proceed as follows:
First we select any nonzero \( r \)-tuple as the first column of the parity check matrix. Then select any non-zero \( r \)-tuple except those that are \( B_1 \) multiples of the first (or \( B_1 \) independent) as the second column in the parity check matrix. The third column may then be any \( r \)-tuple which is not a linear combination of the first and second column, with coefficients from \( B_1 \). In general, the \( i^{th} \) column is chosen as any \( r \)-tuple that is not a linear combination of any \( d - 2 \) or less previous columns with coefficients from \( B_1 \). This construction gives surety that no linear combination of \( d - 1 \) or fewer columns with coefficients from \( B_1 \) will be zero, that is \( d - 1 \) columns will be \( B_1 \)-independent’.

There being \(|B_1|\) possible coefficients, at the time of finding \( j^{th} \) column, the number of \( r \)-tuples to be excluded are

\[
\binom{j-1}{1}|B_1| + \binom{j-1}{2}|B_1|^2 + ... + \binom{j-1}{d-2}|B_1|^{d-2},
\]

the linear combination of \( d - 2 \) or fewer columns out of total of \( j - 1 \) columns. If this is less than total number of non-zero \( r \)-tuples, then there is certainly one more column, the \( j^{th} \), can be added to the matrix. That is, if

\[
1 + \binom{j-1}{1}|B_1| + \binom{j-1}{2}|B_1|^2 + ... + \binom{j-1}{d-2}|B_1|^{d-2} \leq q',
\]

Now let \( n \) be the largest value of \( j \), then an \((n,k)\) code with minimum SK- \( B_1 \)-distance \( d \) is given by

\[
1 + \binom{n}{1}|B_1| + \binom{n}{2}|B_1|^2 + ... + \binom{n}{d-2}|B_1|^{d-2} \geq q',
\]

This proves the result.

**PARTICULAR CASES**

(i) **HAMMING METRIC CASE**

In case of Hamming metric, we have \( m = 2 \), \( B = \{|B_k|,|B_1|\} \), where

\( B_1 = \{1,2,\ldots,q-1\} \) then the expression in Theorem-3.1 can be stated as,
\[ \sum_{i=0}^{d-2} {n\choose i} (q-1)^i \geq q^{n-k}. \]

(ii) **LEE METRIC CASE**

In case of Lee metric, we have \( m-1 = \frac{q-1}{2} \) so, \( B = \left\{ B_0, B_1, \ldots, B_{\frac{q-1}{2}} \right\} \),

\( B_i = \{i, q-i\} \) then expression in Theorem-3.1 takes the form,

\[ \sum_{i=0}^{d-2} {n\choose i} (2)^i \geq q^{n-k}. \]

**BROADENED PARTIAL CASE**

The result of Theorem 3.1 can be further broadened from a single \( B_i \) to that for entries from a group of \( B_i \)'s.

**THEOREM 3.2:** Given an SK-partition \( \mathcal{Q} = \{B_0, B_1, \ldots, B_{m-1}\} \) of \( Z_q \), \( q \) prime, a sufficient condition for the existence of an \( (n,k) \) code over \( Z_q \), with minimum SK-distance at least \( d \) and entries from \( B_1 \) and \( B_2 \), is given by,

\[ \sum_{s=1}^{d-2} \sum_{m=0}^{\left\lfloor \frac{s}{2} \right\rfloor} \binom{n}{s-2m, m, j-s+m-1} |B_1|^{r-2m} |B_2|^m \geq q'. \]

**PROOF:** Let us first consider different linear combinations of length \( n \) with entries from \( B_i \) or \( B_2 \) having SK-weight \( s \). These are given by various columns of the following Table 3.1:

**TABLE - 3.1:** Liner combinations of length \( n \) with entries from \( B_1 \) or \( B_2 \) having SK weight \( s \).

<table>
<thead>
<tr>
<th>Number of entries from ( B_2 )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>...</th>
<th>( M )</th>
<th>...</th>
<th>( s )</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>( \frac{s}{2} )</td>
</tr>
<tr>
<td>Number of entries from ( B_1 )</td>
<td>( s )</td>
<td>( s-2 )</td>
<td>( s-4 )</td>
<td>( s-6 )</td>
<td>...</td>
<td>( s-2m )</td>
<td>...</td>
<td>( s-2 ) ( \frac{s}{2} )</td>
</tr>
<tr>
<td>Number of 0’s</td>
<td>( n-s )</td>
<td>( n-s+1 )</td>
<td>( n-s+2 )</td>
<td>( n-s+3 )</td>
<td>...</td>
<td>( n-s+m )</td>
<td>...</td>
<td>( n-s ) ( \frac{s}{2} )</td>
</tr>
</tbody>
</table>
Then the total number of such \( n \)-vectors is

\[
\begin{align*}
\left( \binom{n}{s,0,(n-s)} |B_1|^s + \binom{n}{s-2,1,(n-s+1)} |B_1|^{s-2}|B_2| + \binom{n}{s-4,2,(n-s+2)} |B_1|^{s-4}|B_2|^2 \right) \\
+ \ldots + \left( \binom{n}{s-2m,m,(n-s+m)} |B_1|^{s-2m}|B_2|^m + \ldots \right) \\
+ \left( \binom{n}{s-2 \left\lfloor \frac{s}{2} \right\rfloor, \left\lfloor \frac{s}{2} \right\rfloor, (n-s+ \left\lfloor \frac{s}{2} \right\rfloor) } |B_1|^{s-2 \left\lfloor \frac{s}{2} \right\rfloor}|B_2|^\left\lfloor \frac{d}{2} \right\rfloor \right)
\end{align*}
\]

\[
= \sum_{m=0}^{\left\lfloor \frac{s}{2} \right\rfloor} \binom{n}{s-2m,m,n-s+m} |B_1|^{s-2m}|B_2|^m.
\]

Now we come to examining the existence of parity-check matrix for the code, as in Theorem 3.1. First we select any nonzero \( r \)-tuple as the first column of the parity check matrix. Then select any non-zero \( r \)-tuple except those that are \( B_1 \) or \( B_2 \) multiples of the first (\( B_1 \) or \( B_2 \) independent) as the second column in the parity check matrix. The third column may then be any \( r \)-tuple which is not a linear combination of the first and second column, with coefficients from \( B_1 \) or \( B_2 \). In general, the \( i^{th} \) column is chosen as any \( r \)-tuple that is not a linear combination of any \( d-2 \) or less previous columns with coefficients from \( B_1 \) or \( B_2 \). This construction give surety that no linear combination of \( d-1 \) or fewer columns with coefficients from \( B_1 \) or \( B_2 \) will be zero, that is \( d-1 \) columns will be \( B_1 \) or \( B_2 \)-independent. There being \( |B_1| \) or \( |B_2| \) possible coefficients, at the time of finding \( j^{th} \) column, the number of \( r \)-tuples to be excluded is

\[
\sum_{m=0}^{\left\lfloor \frac{s}{2} \right\rfloor} \sum_{j=0}^{\left\lfloor \frac{s}{2} \right\rfloor} \binom{n}{s-2m,m,j-1} |B_1|^{s-2m}|B_2|^m,
\]

the linear combination of \( d-2 \) or fewer columns out of total of \( j-1 \) columns. If this is less than total number of non-zero \( r \)-tuples, then there is certainly one more column, the \( j^{th} \), can be added to the matrix. That is, if
Now let \( n \) be the largest value of \( j \), then an \((n,k)\) code with minimum SK-distance \( d \), with entries from \( B_1 \) or \( B_2 \) is given by

\[
\sum_{s=1}^{d-2} \sum_{m=0}^{n-1} \frac{n}{s} \left| B_{s-2m,m,j-s+m-1} \right| B_1^{s-2m} B_2^m \leq q^r,
\]

This proves the result.

**PARTICULAR RESULT**

When \( m = 0 \) then expression in Theorem 3.2 can be written as follows

\[
\sum_{s=1}^{d-2} \sum_{m=0}^{n} \frac{n}{s} \left| B_{s-2m,m,n-s+m} \right| B_1^{s-2m} B_2^m \geq q^r,
\]

which is a particular case when the entries are from \(|B_1|\), the result studied in Theorem 3.1.

**COROLLARY 3.1:** Given an SK-partition \( P = \{B_0, B_1, ..., B_{m-1}\} \) of \( Z_q \), \( q \) prime, a sufficient condition for the existence of an \((n,k)\) code over \( Z_q \), minimum distance at least \( d \), with coefficients from any two partial sets \( B_r \) or \( B_s \), is given by,

\[
\sum_{s=1}^{d-2} \sum_{m=0}^{n} \frac{n}{s} \left| B_{s-2m,m,n-s+m} \right| B_1^{s-2m} B_2^m \geq q^r.
\]

It may be noted that the partial error correction results in reducing the redundancy making search more efficient. In the example below we demonstrate, through an example, that for the
same redundancy $r = 3$ and minimum distance at least $d = 5$, existence of much larger code word length is possible in comparison to the Hamming case of all corrections.

**EXAMPLE 3.1**

Let $Z_q = \{0,1,2,3,4,5,6\}$, $q = 7$ and $r = 3$ then we consider the following two cases:

i. **SK- METRIC CASE:**

Illustrate the results of the Theorem-3.1 considering the SK-partitions of $Z_q$, given by

$$\mathcal{O}_1 = \{B_0, B_1, B_2\},$$

where $B_0 = \{0\}$, $B_1 = \{1,2,5,6\}$ and $B_2 = \{3\}$. For the existence of an $(n,k)$ code over $Z_q$, minimum distance, at least 5, from Theorem 3.1 with coefficients from $B_1$, is given by,

$$4n + \frac{n(n-1)}{2} 16 + \binom{n}{3} \frac{n(n-1)(n-2)}{6} 64 \geq 342$$

\[32n^3 - 72n^2 + 52n \geq 1026\]

The minimum value of $n$ for which it holds is 4. The theorem guarantees existence of a code of minimum length 4, correcting 2 entries obtained by addition of entries in $B_1 = \{1,2,5,6\}$. In actual practice it is possible to try for greater length. In the case of present example, $n = 6$ has been quite possible as is shown by constructing the parity-check matrix given below.

$$
\begin{bmatrix}
100300 \\
010030 \\
001003
\end{bmatrix}
$$
ii. **HAMMING METRIC CASE**

We have to consider the SK-partition.

\[ \varnothing = \{B_0, B_1\}, \]

where \(B_0 = \{0\}\) and \(B_1 = \{1,2,3,4,5,6\}\).

For the existence of an \((n,k)\) code over \(\mathbb{Z}_q\), correcting single error in an \((n, k)\) code with minimum distance \(d = 5\), is given by

\[
\binom{n}{1} + \binom{n}{2} 36 + \binom{n}{3} 216 \geq q^r - 1
\]

\[
6n + 18n(n-1) + 36n(n-1)(n-2) \geq 342
\]

\[
36n^3 - 90n^2 + 60n \geq 342
\]

The minimum value of \(n\) for which it holds is 3 and we get the matrix

\[
\begin{bmatrix}
1 & 0 & 0 & 1 \\
0 & 1 & 0 & 1 \\
0 & 0 & 1 & 1
\end{bmatrix}
\]

### 3.4 CONCLUDING REMARK

The study of the partial error corrections is guided by practical considerations. Here we only considered the existence problem.

In this chapter we have examined the sufficient condition for the existence of a parity check matrix for a given number of parity-checks, obtained an upper bound on number of parity check digits for linear codes with property that correct all partial random error of an \((n,k)\) code with minimum SK-distance at least \(d\). The result generalized the renowned Varshamov-Gilbert bound, which follows from it as a particular case. Results derived under
Hamming considerations follow as particular cases from this study, and those for Lee metric can also be directly obtained.

This is an area for study in actual construction of more efficient codes with designed partial errors.