International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

Blockwise and Low Density Key Error Correcting Codes

Pankaj Kumar Das
Department of Mathematical Sciences, Tezpur University,
Napaam, Sonitpur, Assam-784028, India.
E-mail: pankaj4thapril@yahoo.co.in, pankaj4@tezu.ernet.in

Subodh Kumar
Shyam Lal College, University of Delhi,
G. T. Road Shahdara, Delhi-110032, India.
Corresponding author: subodh05031981@gmail.com

(Received February 21, 2020; Accepted June 29, 2020)

Abstract
To protect the information from disturbances created by noisy channels, redundant symbols (check symbols) with the information symbols are added. These extra symbols play important role for the efficiency of the communication system. It is always important to know how much these check symbols are required for a code designed for a specific purpose. In this communication, we give lower and upper bounds on check symbols needed to a linear code correcting key errors of length upto p which are confined to a single sub-block. We provide two examples of such linear codes. We, further, obtain those bounds for the case when key error occurs in the whole code length, but the number of disturbing components within key error is upto a certain number. Two examples in this case also are provided.

Keywords- Parity check matrix, Syndromes, Bounds, Key errors.

1. Introduction

The main purpose of the coding theorists was to detect and correct the errors which are produced during communication through noisy channels. Communication channels are affected by many external and internal factors that result different types of errors in the messages sent. The coding theorists are always trying to retrieve the message even it is corrupted by various types of errors. Plenty of works have been done by many in this direction. Sharma and Gaur (2013) discussed and studied a different type of error related to the typing on a key board. Their study was on such errors w.r.t. S-K metric (partition). Later this type of error was named as "***key error***" in the work of Das (2014). When a person types on a key board and if by mistake, he presses a different key in the left or right side of the key, then a word with no or different meaning appears. In this case, a key error is created. The definition of a key error given in Das (2014) is as follows:

"*An i-key error of length p is a vector such that the* i^{th} *component is non-zero and the other non-zero component are confined to immediate p consecutive components in either side of the* i^{th} *component.***"**

For example, key errors of length 2 in a vector of length 7 over $GF(3)$ are

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$(\underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{1}\ 020000),\ (2\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{1}\ 22000),\ (20\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{2}\ 0100),\ (22\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{2}\ 2100),\ (0012\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{1}\ 01),$$

$$(00010\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{2}\ 1),\ (00012\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{1}\ 1),\ (000010\ \underset{\substack{\downarrow\\ \text{entry}\\ \text{error}}}{1}\ )\ \text{etc.}$$

According to the definition, the i^{th} position of the vector is always non-zero and other errors can extend up to p^{th} position on both side of the i^{th} position. This means a key error of length may affect $2p+1$ consecutive component. The i^{th} position is called the entry error position of the i-key error. When the entry error position can take any place within the code length (or sub-block of code length), we simply call the error as *key error*.

Detection of key error is studied by Das (2014) and correction of key error is taken care of by Das (2015). A midway concept between detection and correction (called error location), was initiated by Wolf and Elspas (1963). Location and weight distribution of key error are discussed by Das and Kumar (2020). In continuation with the study of key error, in this paper, we have considered the following two cases:

(i) when the length of the code is divided into some smaller length mutually exclusive sub-blocks and key error occurs within a single sub-block.
(ii) when key error occurs in whole code length, but with low density, i.e., maximum number of disturbed components within key error should be less than a limit, called low density key error.

The case (*i*) is considered keeping in mind the situation when sub-blocks are independent and a corrupted sub-block with key error does not affect other sub-blocks. This is the extension work of location of key error (Das and Kumar, 2020) to correction of key error occurring within a sub-block. In (Das and Kumar, 2020), location of key error was possible, but the correction of such error was not possible. In this paper, we present this case, i.e., to correct key errors of length upto p within any single sub-block of length (say) t. We present Single Blockwise Key Error (of length upto p within a sub-block of length t) Correcting Codes. We denote such codes by $\boldsymbol{SBKE_{p/t}C}$ **codes**. We obtain lower as well as upper bounds on number of check symbols (redundant symbols) of such $\boldsymbol{SBKE_{p/t}C}$ **codes**.

The case (*ii*) is considered when key error occurs in the whole code length and certain number or less components within the key error get disturbed. The possibility of certain number or less components getting disturbed is more likely than all components within key errors. Consideration of such situation is initiated by Wyner (1963). In view of this, we present here the lower as well as the upper bounds on number of check symbols for linear codes that are capable to correct key error of length upto p with hamming weight ω or fewer ($\omega \leq 2p + 1$) in the whole code length. We denote such codes by $\boldsymbol{K_{\omega,p}EC}$ **codes**.

The number of check symbols (or redundant symbols) of a code is important because the rate of information increases if the number of check symbols is lesser and decreases if the number is more. The bounds on number of check symbols (redundant symbols) tell us the limitation and capability of error detection and correction of a code.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

The rest of the paper is written as follows. In Section 2, we derive lower as well as upper bounds on the number of check symbols for a ***SBKE$_{p/t}$C* code** and then we give two examples of such codes. In Section 3, similar bounds for a ***K$_{\omega,p}$EC* code** are obtained. This is also followed by two examples. At the end, conclusion is given.

2. Correction of Key Errors Blockwise

We, in this section, first provide the lower number and then the upper number of check (redundant) symbols required for the linear codes which can correct key errors blockwise. The section ends with two examples of such codes.

Theorem 2.1 *For an (n = ft, n-r) **SBKE$_{p/t}$C code** over finite field F_q having r check symbols, the value of r must be at least*

$$\log\left[1+ f\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right].$$

Proof. We prove this theorem by enumerating the total number of correctable errors occurring in *f* sub-blocks each of length *t*. From Das (2015), the total number of correctable errors in a *t*-tuple is

$$\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}.$$

.

Since the code has *f* sub-blocks of length *t*, therefore the total number of correctable errors occurring in all *f* sub-blocks is

$$f\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}.$$

Hence

$$q^r \geq 1+ f\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}.$$

Remark 2.2 For *f* = 1, Theorem 2.1 coincides with Theorem 2.1 (Das, 2015) for code length $n = t$.

For the upper bound, we follow the method of well-known Varshaomov-Gilbert-Sacks bound ((Sacks, 1958) , Theorem 4.7 (Peterson and Weldon, 1972)).

Theorem 2.3 *An (n = ft, n-r) **SBKE$_{p/t}$C code** ($t > 4p+1$) over finite field F_q having r check symbols shall always exist provided*

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$q^r > \frac{1+q^{2p+1}}{1+q}\left[\left\{1+\frac{q^{2p+1}-q}{1+q}+\left\{(t-4p-1)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right.$$
$$\left.+(f-1)\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right].$$

Proof. To prove this theorem, we construct a suitable parity check matrix *H* of order $r\times n$ for the ***SBKE$_{p/t}$C*** code in need. Let us assume that the initial $f-1$ sub-blocks of *H* and the initial $\tau-1$ columns $h_1, h_2, h_3, h_4, \ldots, h_{\tau-1}$ of the f^{th} sub-block of *H* are selected appropriately. Then, we add the τ^{th} column h_τ of f^{th} sub-block by the two following conditions:

$$h_\tau \neq (u_1h_{\tau-1}+u_2h_{\tau-2}+\cdots+u_{2p}h_{\tau-2p})+(v_lh_l+v_{l+1}h_{l+1}+\cdots+v_{l+2p}h_{l+2p}), \quad (1)$$

where $u_i, v_i \in GF(q)$; $l+2p<\tau-2p$; the coefficient u_i's are such that $\{h_{\tau-2p}, h_{\tau-2p+1},..., h_{\tau-1}, h_\tau\}$ form a key error of length upto *p* and the coefficient v_i's are such that $\{h_l, h_{l+1},... h_{l+2p-1}, h_{l+2p}\}$ (where $l=1,2,\ldots,\tau-4p-1$) form any key error of length upto *p* in the first $\tau-2p-1$ columns of the f^{th} sub-block.

and

$$h_\tau \neq (u_1h_{\tau-1}+u_2h_{\tau-2}+\cdots+u_{2p}h_{\tau-2p})+(w_lh_l+w_{l+1}h_{l+1}+\cdots+w_{l+2p}h_{l+2p}), \quad (2)$$

where $u_i, w_i \in GF(q)$, the coefficient u_i's are such that $\{h_{\tau-2p}, h_{\tau-2p+1},..., h_{\tau-1}, h_\tau\}$ form a key error of length upto *p* and the coefficient w_i's are such that $\{h_l, h_{l+1},... h_{l+2p-1}, h_{l+2p}\}$ (where $l=1,2,\ldots,t-2p$) form a key error of length upto *p* in any *other* sub-block.

From Das (2015), the total number of coefficients u_i's and v_i's in expressions (1) is given by respectively

$$\frac{1+q^{2p+1}}{1+q}$$

and

$$1+\frac{q^{2p+1}-q}{1+q}+\left\{(\tau-4p-1)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}.$$

So, the total number of u_i's and v_i's on the expression (1) is given by

$$\frac{1+q^{2p+1}}{1+q}\left\{1+\frac{q^{2p+1}-q}{1+q}+\left\{(\tau-4p-1)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}. \quad (3)$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

Now, the computation of coefficients w_i's on R. H. S. of (2) is equivalent to finding key errors of length upto p in a vector of length t, which is given by

$$\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}.$$

As the number of sub-blocks is $f-1$, so, the total number of coefficient w_i's in (2) is

$$(f-1)\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}. \tag{4}$$

Hence, the total number of u_i's and w_i's in expression (2) is given by

$$(f-1)\left(\frac{1+q^{2p+1}}{1+q}\right)\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}. \tag{5}$$

Thus, the total number of linear sums due to expression (1) and (2) is

$$Expr:(3)+Expr:(5)$$

i.e.

$$\left(\frac{1+q^{2p+1}}{1+q}\right)\left[\left\{1+\frac{q^{2p+1}-q}{1+q}+\left\{(\tau-4p-1)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right.$$
$$\left.+(f-1)\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right].$$

Now, putting this number less than q^r, we get

$$q^r>\left(\frac{1+q^{2p+1}}{1+q}\right)\left[\left\{1+\frac{q^{2p+1}-q}{1+q}+\left\{(\tau-4p-1)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right.$$
$$\left.+(f-1)\left\{\frac{q^{2p+1}-q}{1+q}+\left\{(t-2p)(1+q^{2p+1})+q+p\right\}\frac{q-1}{1+q}+\frac{q^{2p+1}-q^3}{(1+q)^2}\right\}\right].$$

By replacing τ by t, we get the required result.

Remark 2.4 For f = 1, Theorem 2.3 coincides with Theorem 2.2 (Das, 2015) for code length $n = t$.

Now, we give two examples of codes in support of our results derived above. In the first, we give an example in binary case which is followed by an example in ternary case.

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

Example 2.5 Taking q = 2, p = 2, t=*11*, f = 4 in Theorem 2.3, we get $r > 10$. This gives rise to a binary (44, 32) linear code. The parity check matrix H of order 12×44 of this code is constructed by the synthesis procedure discussed in Theorem 2.3 and is given below.

$$H = \begin{bmatrix}
10000000000 & 01111111111 & 11111111111 & 11111111111 \\
01000000000 & 01001111011 & 11111100100 & 01100110010 \\
00100000000 & 01100111001 & 11000010011 & 00001000011 \\
00010000000 & 01011011000 & 11000011110 & 11111000100 \\
00001000000 & 01101001110 & 01000101001 & 01011101101 \\
00000100000 & 01000100010 & 00100111110 & 10100111011 \\
00000010000 & 01111100000 & 00110010110 & 11101001110 \\
00000001000 & 01001110001 & 01011010101 & 01001010101 \\
00000000100 & 01100010111 & 00001100010 & 10111010011 \\
00000000010 & 01011011011 & 10000111100 & 00010101010 \\
00000000001 & 01101111000 & 11100111011 & 01111110111 \\
00000000000 & 11000101000 & 11101111110 & 11101111111
\end{bmatrix}$$

All the 364 key errors of length upto p = 2 occurring in the same sub-block or in different sub-block and the corresponding syndromes for this code can be obtained with the help of MS-EXCEL and it is verified that the syndromes are all non-zero and distinct. So, this is a ***SBKE$_{2/11}$C codes in binary case.***

Example 2.6 Taking q = 3, p = 2, f = 2, t=*11* in Theorem 2.3, we get a ternary (22, 11) linear code and its parity check matrix is given by

$$H = \begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0 & 1&1&1&1&1&1&1&1&0&1&1 \\
0&1&0&0&0&0&0&0&0&0&0 & 1&0&0&1&2&1&1&0&1&2&0 \\
0&0&1&0&0&0&0&0&0&0&0 & 1&2&0&0&1&1&2&0&0&1&2 \\
0&0&0&1&0&0&0&0&0&0&0 & 1&0&2&1&0&1&1&0&0&0&0 \\
0&0&0&0&1&0&0&0&0&0&0 & 1&1&0&1&0&0&1&2&2&0&0 \\
0&0&0&0&0&1&0&0&0&0&0 & 1&0&0&0&2&0&0&0&1&0&2 \\
0&0&0&0&0&0&1&0&0&0&0 & 1&2&1&1&1&0&0&2&0&0&0 \\
0&0&0&0&0&0&0&1&0&0&0 & 1&0&0&1&1&1&0&0&0&1&0 \\
0&0&0&0&0&0&0&0&1&0&0 & 1&1&0&0&0&2&0&1&1&1&0 \\
0&0&0&0&0&0&0&0&0&1&0 & 1&0&1&1&0&2&1&0&0&2&1 \\
0&0&0&0&0&0&0&0&0&0&1 & 1&1&0&0&0&1&1&2&2&0&0
\end{bmatrix}.$$

We can verify that all the syndromes of key errors of length upto 2 occurring in same sub-block or different sub-block are non-zero and distinct. So, this is a ternary ***SBKE$_{2/11}$C code.***

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

3. Correction of Low Density Key Errors

In Das (2014), correction of key errors of length upto p occurring in the whole code length is studied. Motivated by Wyner (1963), we consider key errors of length upto p with hamming weight ω or fewer in the whole code length and correction of such errors is studied in this section. We obtain analogous bounds as presented in Section 2 and we end this section with two examples of such codes. First, we give the following identity which is used for simplification of calculation of our results. The identity can be proved easily with Pascal Formula (Balakrishnan, 1996).

Identity 3.1 For non-negative integers n, m and p with $n \geq m$,

$$\binom{n}{m}+\binom{n+1}{m}+\binom{n+2}{m}+\cdots+\binom{n+p}{m}=\binom{n+p+1}{m+1}-\binom{n}{m+1}.$$

For the following two results, we assume that $\binom{n}{m}=0$ if n is negative integer or smaller than m.

Theorem 3.1 *For an (n, n-r)* $\boldsymbol{K_{\omega,p}EC}$ *code over finite field* F_q *having r check symbols, the following inequality must be satisfied*

$$q^r \geq 1+\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}$$
$$+(n-2p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$
$$+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1).$$

Proof. For the proof, we count the number of key errors of length upto p with hamming weight ω or fewer in the following way.

When the entry error position is from 1st to p^{th} position, the number of key errors of length upto p with hamming weight ω or fewer is calculated as

$$\sum_{\alpha=0}^{\omega-1}\binom{p}{\alpha}(q-1)^{1+\alpha}+\left[\sum_{\alpha=0}^{\omega-2}\binom{p}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\binom{p-1}{\alpha}(q-1)^{1+\alpha}\right]$$
$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{p+1}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{p-1}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\binom{p-2}{\alpha}(q-1)^{1+\alpha}\right]$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{p+2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{p}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{p-2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\binom{p-3}{\alpha}(q-1)^{1+\alpha}\right]$$
$$\vdots$$
$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{2p-2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-4}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-6}{\alpha}(q-1)^{2+\alpha}+\cdots\right.$$
$$\left.+\sum_{\alpha=0}^{\omega-2}\binom{2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\binom{1}{\alpha}(q-1)^{1+\alpha}\right],$$

i.e.

$$\sum_{\alpha=0}^{\omega-2}\left[\binom{p}{\alpha}+\binom{p+1}{\alpha}+\binom{p+2}{\alpha}+\cdots+\binom{2p-2}{\alpha}\right](q-1)^{2+\alpha}$$
$$+\sum_{\alpha=0}^{\omega-2}\left[\binom{p-1}{\alpha}+\binom{p}{\alpha}+\binom{p+1}{\alpha}+\cdots+\binom{2p-4}{\alpha}\right](q-1)^{2+\alpha}$$
$$+\sum_{\alpha=0}^{\omega-2}\left[\binom{p-2}{\alpha}+\binom{p-1}{\alpha}+\binom{p}{\alpha}+\cdots+\binom{2p-6}{\alpha}\right](q-1)^{2+\alpha}$$
$$\vdots$$
$$+\sum_{\alpha=0}^{\omega-2}\left[\binom{2}{\alpha}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p}{\alpha}+\binom{p-1}{\alpha}+\binom{p-2}{\alpha}+\cdots+\binom{1}{\alpha}\right](q-1)^{1+\alpha}.$$

This, after applying Identity 3.1, simplifies to

$$\sum_{\alpha=0}^{\omega-2}\left[\binom{2p-1}{\alpha+1}-\binom{p}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\left[\binom{2p-3}{\alpha+1}-\binom{p-1}{\alpha+1}\right](q-1)^{2+\alpha}$$
$$+\sum_{\alpha=0}^{\omega-2}\left[\binom{2p-5}{\alpha+1}-\binom{p-2}{\alpha+1}\right](q-1)^{2+\alpha}+\cdots+\sum_{\alpha=0}^{\omega-2}\left[\binom{3}{\alpha+1}-\binom{2}{\alpha+1}\right](q-1)^{2+\alpha}$$
$$+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}$$
$$=\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta-1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}. \quad (6)$$

When the entry error position is taken from $(p+1)^{\text{th}}$ upto $(n-p)^{\text{th}}$ position, the number of key errors of length upto p with hamming weight ω or fewer is

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$(n-2p)\left\{\sum_{\alpha=0}^{\omega-2}\binom{2p-1}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-3}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-5}{\alpha}(q-1)^{2+\alpha}+\cdots\right.$$
$$\left.+\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$
$$=(n-2p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}. \quad (7)$$

Similarly, when the entry error position is considered in the last p components, the number of such key errors is

$$\left[\sum_{\alpha=0}^{\omega-2}\binom{2p-3}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-5}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-7}{\alpha}(q-1)^{2+\alpha}+\cdots\right.$$
$$\left.+\sum_{\alpha=0}^{\omega-2}\binom{3}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right]$$
$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{2p-5}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-7}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{2p-9}{\alpha}(q-1)^{2+\alpha}+\cdots\right.$$
$$\left.+\sum_{\alpha=0}^{\omega-2}\binom{3}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right]$$
$$\vdots$$
$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{5}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{3}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right]$$
$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{3}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right]$$
$$+\left[\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right]+(q-1),$$

i.e.

$$\left[\sum_{\alpha=0}^{\omega-2}\binom{2p-3}{\alpha}(q-1)^{2+\alpha}+2\sum_{\alpha=0}^{\omega-2}\binom{2p-5}{\alpha}(q-1)^{2+\alpha}+3\sum_{\alpha=0}^{\omega-2}\binom{2p-7}{\alpha}(q-1)^{2+\alpha}+\cdots\right.$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$+(p-2)\sum_{\alpha=0}^{\omega-2}\binom{3}{\alpha}(q-1)^{2+\alpha}+(p-1)\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{2+\alpha}+p(q-1)\Bigg]$$

$$=\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1). \tag{8}$$

Therefore, the total number of key errors of length upto p with hamming weight ω or fewer is given by

$$Expr:(6)+Expr:(7)+Expr:(8)$$

$$=\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}$$

$$+(n-2p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$

$$+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1). \tag{9}$$

For correction, this number must be greater than or equal to q^r. Therefore, we must have

$$q^r\geq 1+\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}$$

$$+(n-2p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$

$$+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1). \tag{10}$$

Remark 3.2 For $p = 0$, the maximum value of ω is 1. Then, the key errors of length $p = 0$ with hamming weight $\omega = 1$ or fewer will be the all single errors. Putting $p = 0$ and $\omega = 1$ in the inequality (10), we have

$$q^r\geq 1+n(q-1).$$

This coincides with the famous Hamming's Sphere-Packing bound (Hamming, 1950; also Peterson and Weldon, 1972) for single errors. This is the necessary condition to be satisfied for any single error correcting linear code.

Theorem 3.3 *An (n, n-r)* $\boldsymbol{K_{\omega,p}EC}$ *code* $(\omega\leq 2p+1, n>4p+2)$ *over finite field* F_q *having r check symbols shall always exist provided that*

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$q^r > \left\{\sum_{\alpha=0}^{\omega-3}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}+1\right\}$$
$$\times\left\{1+\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}\right.$$
$$+(n-1-4p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$
$$\left.+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1)\right\}.$$

Proof. For construction of parity check matrix H of order $r\times n$ for the desired $\boldsymbol{K_{\omega,p}EC}$ code, we follow the synthesis procedure as followed in Theorem 2.3. We take any nonzero r-tuple as the first column h_1 of the matrix H and for selection of next $\tau-1$ columns $h_2, h_3, h_4, \ldots., h_{\tau-1}, h_\tau$ one by one, we follow the condition:

$$h_\tau \neq (u_1h_{\tau-1}+u_2h_{\tau-2}+\cdots+u_{2p}h_{\tau-2p})+(v_lh_l+v_{l+1}h_{l+1}+\cdots+v_{l+2p}h_{l+2p}), \tag{11}$$

where $u_i, v_i \in GF(q)$; $l+2p<\tau-2p$; the coefficient u_i's are such that $\{h_{\tau-2p}, h_{\tau-2p+1},.., h_{\tau-1}, h_\tau\}$ form a key error of length upto p with the condition that the number of non-zero coefficients u_i's should not exceed ω and the coefficient v_i's are such that $\{h_l, h_{l+1},\ldots,h_{l+2p}\}$, $(l=1,2,\ldots,\tau-4p-1)$ form a key error of length upto p with hamming weight ω or fewer in the first $\tau-2p-1$ columns of H.

We now calculate the total number of all possible linear sums on the R.H.S. of (11):

The number of coefficients u_i's, including the zero vector, is calculated as

$$\sum_{\alpha=0}^{\omega-2}\binom{p}{\alpha}(q-1)^{1+\alpha}$$
$$+\left[\sum_{\alpha=0}^{\omega-3}\binom{p}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{p-1}{\alpha}(q-1)^{1+\alpha}\right]$$
$$+\left[\sum_{\alpha=0}^{\omega-3}\binom{p+1}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-3}\binom{p-1}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{p-2}{\alpha}(q-1)^{1+\alpha}\right]$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

$$+\left[\sum_{\alpha=0}^{\omega-3}\binom{p+2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-3}\binom{p}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-3}\binom{p-2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{p-3}{\alpha}(q-1)^{1+\alpha}\right]$$

$$\vdots$$

$$+\left[\sum_{\alpha=0}^{\omega-3}\binom{2p-2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-3}\binom{2p-4}{\alpha}(q-1)^{2+\alpha}+\cdots+\sum_{\alpha=0}^{\omega-3}\binom{2}{\alpha}(q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\binom{1}{\alpha}(q-1)^{1+\alpha}\right]+1,$$

which can be written as (by using Identity 3.1)

$$\sum_{\alpha=0}^{\omega-3}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}+1. \quad (12)$$

The number of the coefficients v_i is equal to the number of key errors of length upto p with hamming weight ω or fewer in a $(\tau-1-2p)$-tuple. This number, including the vector of all zero components, is computed in (9), i.e.

$$\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}$$

$$+(\tau-1-4p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$

$$+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1). \quad (13)$$

Therefore, the total number of linear sums on R.H.S. of (11) is equal to

$Expr:(12)\times Expr:(13)$

$$=\left\{\sum_{\alpha=0}^{\omega-3}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}+1\right\}$$

$$\times\left\{1+\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}\right.$$

$$+(\tau-1-4p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$

$$\left.+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1)\right\}. \quad (14)$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

Since the available number of *r*-tuples is q^r, so the addition of the τ^{th} column h_τ to *H* is possible provided

$$q^r > Expr:(14).$$

For a code of length *n*, we need to replace τ by *n* and we get

$$q^r > \left\{\sum_{\alpha=0}^{\omega-3}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-2}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}+1\right\}$$
$$\times\left\{1+\sum_{\alpha=0}^{\omega-2}\sum_{\eta=1}^{p-1}\left[\binom{2\eta+1}{\alpha+1}-\binom{\eta+1}{\alpha+1}\right](q-1)^{2+\alpha}+\sum_{\alpha=0}^{\omega-1}\left[\binom{p+1}{\alpha+1}-\binom{1}{\alpha+1}\right](q-1)^{1+\alpha}\right.$$
$$+(n-1-4p)\left\{\sum_{\alpha=0}^{\omega-2}\sum_{\gamma=0}^{p-1}\binom{2\gamma+1}{\alpha}(q-1)^{2+\alpha}+(q-1)\right\}$$
$$\left.+\sum_{\alpha=0}^{\omega-2}\sum_{\mu=0}^{p-2}(p-1-\mu)\binom{2\mu+1}{\alpha}(q-1)^{2+\alpha}+p(q-1)\right\}. \quad (15)$$

Remark 3.4 For $p = 0$ and $\omega = 1$, the inequality (15) reduces to

$$q^r > 1+(n-1)(q-1)=\sum_{\alpha=0}^{1}\binom{n-1}{\alpha}(q-1)^{\alpha}.$$

This coincides with the famous Varsharmov-Gilbert-Sacks bound (Sacks, 1958; Peterson and Weldon, 1972) for single errors. This is the sufficient condition for existing single error correcting linear code.

In this case also, we provide two examples of codes: one for binary case and one for ternary case.

Example 3.5 Taking $n = 11$, $q = 2$, $p = 2$ and $\omega = 3$ in Theorem 3.3, we get a binary (11, 3) linear code whose parity check matrix *H* is constructed by the method discussed in the theorem:

$$H=\begin{bmatrix}1&0&0&0&0&0&0&0&1&1&1\\0&1&0&0&0&0&0&0&1&1&0\\0&0&1&0&0&0&0&0&1&0&0\\0&0&0&1&0&0&0&0&1&1&1\\0&0&0&0&1&0&0&0&1&1&0\\0&0&0&0&0&1&0&0&1&0&0\\0&0&0&0&0&0&1&0&1&1&1\\0&0&0&0&0&0&0&1&1&1&0\end{bmatrix}.$$

International Journal of Mathematical, Engineering and Management Sciences
Vol. 5, No. 6, 1234-1248, 2020
https://doi.org/10.33889/IJMEMS.2020.5.6.092

All 62 key errors of length upto $p = 2$ with hamming weight 3 or fewer and their corresponding syndromes code can be obtained with the help of MS-EXCEL and the syndromes are found to be nonzero and distinct. Therefore, the above code is a binary $\boldsymbol{K_{3,2}EC}$ *code*.

Example 3.6 $n = 11$, $q = 3$, $p = 2$ and $\omega = 3$ in Theorem 3.3 give rise to a (11, 3) linear code. The parity check matrix H of this code is given by

$$H = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 2 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 \end{bmatrix}.$$

Syndromes of all key errors of length upto 2 with hamming weight 3 or fewer are found to be nonzero and distinct. Therefore, the above code is a ternary (11, 3) $\boldsymbol{K_{3,2}EC}$ *code*.

4. Conclusion

This paper derives lower as well as upper number of check symbols needed to exist linear codes that correct all the key errors occurring within a sub-block. Further, such bounds for codes correcting low density key errors are also obtained. The numerical examples are given to justify the results. They give us the surety that the information rate for the codes is always achievable at least a certain limit. Correcting key errors in more than one sub-block (i.e., in multiple sub-blocks) remains to be studied.

Conflict of Interest
The authors declare that they have no conflict of interest.

Acknowledgement
The authors like to thank the editor and referees for careful review of the manuscript and helpful comments.

References

Balakrishnan, V.K. (1996). *Introductory discrete mathematics*. Dover Publications, New York.

Das, P.K. (2014). Codes on key errors. *Cybernetics and Information Technologies, 14*(2), 31-37.

Das, P.K. (2015). Codes correcting key errors. *TWMS Journal of Applied and Engineering Mathematics*, *5*(1), 110-117.

Das, P.K., & Kumar, S. (2020). Location and weight distribution of key errors. *Accepted for Publication in Matematiki Vesnik.*

Hamming, R.W. (1950). Error detecting and error correcting codes. *The Bell System Technical Journal*, *29*(2), 147-160.

Peterson, W.W., & Weldon Jr, E.J. (1972). Error-correcting codes, 2nd edition. *MIT Press, Cambridge, MA*.

Sacks, G.E. (1958). Multiple error correction by means of parity checks. *IRE Transactions on Information Theory*, *4*(4), 145-147.

Sharma, B.D., & Gaur, A. (2013). Codes correcting limited patterns of random errors using SK metric. *Cybernetics and Information Technologies*, *13*(1), 34-45.

Wolf, J.K., & Elspas, B. (1963). Error-locating codes-a new concept in error control. *IEEE Transanction on Information Theory*, *9*(2), 20-28.

Wyner, A.D. (1963). Low-density-burst-correcting codes. *IEEE Transactions on Information Theory*, *9*(2), 124-124.