Detection and Location of Restricted Key Errors

Subodh Kumar[1], Hari Pratap[2*], Manoj Kumar[3], Gajraj Singh[4], Niti Agrawal[5]

[1]Department of Mathematics, Shyam Lal College, University of Delhi, India
[2]Department of Mathematics, PGDAV (E) College, University of Delhi, India.
[3]Department of Mathematics, Deshbandhu College, University of Delhi, India.
[4]Discipline of Statistics, Indira Gandhi National Open University, Delhi, India
[5] Department of Physics, Shyam Lal College, University of Delhi, India

[1]skumarmath@shyamlal.du.ac.in, [3]manojccs@gmail.com,
[4]gajrajsingh@ignou.ac.in, [5]nagrawal@shyamlal.du.ac.in
[*]Corresponding Author, [2]haripratap@pgdave.du.ac.in

Received: 05.03.2024 Revised: 12.05.2024 Accepted: 18.06.2024

ABSTRACT
A new type of errors known as restricted key error is introduced through this paper. Some formulae's are provided to calculate the restricted key errors occurred in a vector of given length over $GF(q)$. Also, Bounds on the check symbols needed for codes to be able to detect and locate restricted key errors that occur anywhere throughout the code length have been derived.

Keywords: Restricted key errors (RK errors), Detection, Correction, Codes, Parity check matrix (PCM), Error patterns, Syndromes

Subject Classification [2010]: 94B05, 94B65

1. INTRODUCTION

There is a large number of communication channels that are being used to send information from one place to another place. Each channel has a specific speed to transmit a particular type of information in the form of signals. During the transmission of a message through a channel, there may occur any error and the receiver may be unable to find the actual massage that was sent. There are several types of errors like random error, burst errors, repeated bust errors and key errors. Any message is sent in the form of strings of numbers or vectors. When due to a faulty channel, any digit of a string is replaced by any other digit at random basis, then such type of occurrence of error is called a random error. When some successive digits of a string are replaced by other digits then this clustered replacement is called a burst [9]. In the heavy loaded communication channels a burst error can repeat itself in a vector then such error is called repeated burst error [2, 8]. In the paper [13], the author introduced restricted burst errors. The paper [1] gives the repeated restricted burst errors with bounds for the codes capable to correct these repeated restricted burst errors. At first, the key error was introduced by P. K. Das [4]. When a person uses the keyboard while working on a computer and accidentally presses a wrong key, a different word that is meaningless or with different meaning appears. Due to this reason, Das named such error as a key error. The key that supposed to be pressed is referred to as \textit{entry error} of the key error. The entry error is always considered to be non-zero.

According to Das a key error is defined as “An i-key error of length b (i = 1, 2,…, n) is an n-tuple such that the *i*th component is non-zero and all other nonzero components are confined upto b consecutive positions (if exist) immediately preceding and succeeding the *i*th component” in [4], the author obtained the codes that correct the key errors.

By introducing the idea of error locating codes, Wolf [14] proposed a midway approach to error detection and correction of the various types of errors.The paper [5] gives the codes that can locate the key errors and also suggested the weight distribution of the key errors. In the paper [6], the codes are developed that are capable to deal with the key errors existing in a sub-block. Such a code is divided into a predetermined number of sub-blocks that are mutually exclusive.

A code is considered to be a good code if it possess more information digits. Such codes help to enhance the efficiency of a channel. Aiming the reduction of the check digits of a code, we are introducing a new type of errors which will be known as restricted key errors (RK errors).

Definition 1.1 A restricted *i*-key error of length is a vector over *GF*(*q*) in which all the non-zero components occur only at β or less consecutive positions either or both sides of *i*th position. The last component of each side is non-zero and each non-zero component is same element of *GF*(*q*). The *i*th component is called entry error of the restricted key.

2. CALCULATION OF RESTRICTED KEY ERROS OCCURRING IN A VECTOR

We can calculate the restricted key errors of length β or less occuring in a vector of length *n* by imposing the restriction over the non-zero components of the key errors obtained by P. K Das in his paper [4] . We can determine the restricted key errors from the key errors if the number $(q-1)$ is multiplied to the number of key errors for binary case in each corresponding case of Theorem 2.1 of [4]. In the similar manner as the key errors the RK errors are divided into three parts:

(a). If the entry error varies from first position to β^{th} position, then total number of restricted key errors is given by

$$\frac{2}{3}(q-1)\left(2^{2\beta}-1\right). \tag{2.1}$$

(b). If the entry error shifts from $(\beta+1)^{th}$ to $(n-\beta)^{th}$ position. Afterwards, the total count of RK errors is provided by

$$\frac{(n-2\beta)}{3}(q-1)\left(2^{(2\beta+1)}+1\right). \tag{2.2}$$

(c). If the entry error lies between the β^{th} and n^{th} positions. Then the number of total restricted key errors is given by

$$(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]. \tag{2.3}$$

Consequently, the sum of RK errors of length upto β that occur in an *n* tuple is provided by

Expr (2.1)+Expr (2.2)+Expr (2.3)

i.e.

$$(q-1)\left[\frac{2}{3}\left(2^{2\beta}-1\right)+\frac{(n-2\beta)}{3}\left(2^{(2\beta+1)}+1\right)+\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]. \qquad (2.4)$$

3. DETECTION OF RESTRICTED KEY ERRORS

In the present section , the necessary and sufficient conditions to detect restricted key errors by a code will be derived. The occurrence of the restricted key errors is considered to be in whole code length. For the restricted key errors detecting codes, the syndromes of the RK errors satisfy the following conditions.

(i) The syndromes corresponding to the RK errors corresponding to all possible restricted key errors must be different from zero vector.

Theorem 3.1 The number of parity check digits for a (*n, k*) code over *GF(q)* must satisfy the following condition in order to detect restricted key errors of length β or less that occur throughout the code length.

$$q^{n-k}\geq 1+\frac{(q-1)}{3}\left(2^{(2\beta+1)}+1\right).$$

Proof. This result can be derived by determining the number of all possible restricted key errors that have to be detected.

Let us assume that *L* represents the set of all those vectors having their all non-zero restricted entries lying in the first $2\beta+1$ position. We ensure that these vectors (restricted key errors) are distinct or we can say that no two different restricted key errors occur in the same coset. To prove our claim, we assume that two different restricted key errors *E₁* and *E₂* are in the one coset. As sum or difference of two restricted key errors is a code vector. But by our assumption, $E_1 + E_2$ or $E_1 - E_2$ is an element of *L*, that concludes a contradiction. Therefore, our claim is proved.

The number of all possible elemnts in *L* is equivalent to the number of restricted key errors in a vector when the entry error varies from first position to $(\beta+1)^{th}$ position.

i.e.

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

or

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

Therefore the following number gives the total number of the RK erros that have to be detected (taking the all zero vector together).

$$1+\frac{(q-1)}{3}\left(2^{2(\beta+1)}-1\right) \qquad (3.1)$$

We can obtain the desired resurt by taking expression (3.1)< q^{n-k}, where q^{n-k} is the number of all possible cosets.

i.e.

$$q^{n-k} \geq 1+\frac{(q-1)}{3}\left(2^{2(\beta+1)}-1\right).$$

In the following theorem, we will prove the sufficient condition required to exist a code that can detect the RK errors in the whole code length. The famous bound, Varshamov-Gilbert-Sacks Bound (VGS Bound) (refer Theorem 16.14, [8]) will be used to prove this theorem. This bound provides a technique to construct a PC matrix for codes. This theorem is verified by giving an example.

Theorem 3.2. The construction of a PC matrix is possible that ensures the existence of an (*n, k*) code over *GF*(*q*) capable to detect the restricted key errors of length β or less if the following condition is satisfied.

$$q^{n-k} > 1+(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right].$$

Proof. The existence of the codes capable to locate the restricted key errors in a single sub-block is considered to be ensured if the construction of a PC matrix *H* for such codes is done. This task will be performed by using the VGS Bound. As per this bound, let us choose appropriate *n-k* tuples over *GF*(*q*) to make all the columns of the first $f-1$ sub-blocks together with the first $\rho-1$ columns of the f^{th} sub-block of *H*.

In accordance with condition (i), if column h_ρ is not a linear sum of the 2β or fewer columns just preceding ρ, then the ρ^{th} column h_ρ of the PC matrix *H* can be added.

i.e.,

$$h_\rho \neq u_1h_{\rho-1}+u_2h_{\rho-2}+u_3h_{\rho-3}+.\cdots+u_\beta h_{\rho-\beta}, \tag{3.2}$$

where u_i,s are same field elements of *GF*(*q*). In expression (3.2), the calculation of the u_i,s coefficients is same as the calculation of the number of the RK errors occurring in last β possition of a vector, which is given by

$$(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]$$

Due to the expression (3.2) the total number of l.c. (taking together the *n-k* tuple with all zero components) that is not equal to h_ρ is given by

$$1+(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right].$$

The required result will be obtained by putting this expression less than q^{n-k}.

i.e.

$$q^{n-k} > 1 + (q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)} - 1\right) + \frac{\beta+2}{3}\right].$$

To wrap up this section, An example of the code that can detect RK errors up to β in length is provided.

Example 3.3. Taking $q = 3$, $\beta = 2$, $n = 10$ in Theorem 3.2 in Theorem 3.2, a ternary (10, 7) linear code is obtained whose PCM is as follows:

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

The error patterns syndrome table for this PC matrix can be made easily by using MS-EXCEL. The syndromes due to the RK error with lengths up to 2 that occur throughout the entire code length are non-zero. So, this ternary code is capable to detect the key errors of length upto 2.

4. LOCATION OF THE RESTRICTED KEY ERRORS

We are going to establish bounds over the check digits for a code that gives us information where the restricted key errors are located. It is assumed that the entire code length of the codes that are able to lacate the RK errors is separated into a predetermined number of equally long sub-blocks that are mutually exclusive. The syndromes of the RK errors satisfy the conditions given below.

(i) The Syndromes of each sub-block that correspond to the RK errors must differ from the zero vector.

(ii) There must be a difference between the syndromes due to the RK errors in one sub-block and the syndromes due the RK errors in any other sub-block.

Theorem 4.1. The following condition must be met in order to locate the restricted key errors of length β in a single sub-block of a $(n = fl, k)$ code over *GF*(*q*) with *k* information digits and entire code length is split up into f sub-blocks, each with a length of *l* and mutual exclusivity.

$$q^{n-k} \geq 1 + \frac{f(q-1)}{3}\left(2^{2(\beta+1)} - 1\right).$$

Proof. To derive this result we will determine the number of all possible restricted key errors that have to be located.\\

Since there are a total of f sub-blocks, the expression (3.1) indicates the number of possible restricted key errors that can occur in a single sub-block. Consequently, the number of all possible RK errors (including the all zero component vector) that need to be located is given by

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

(4.1)

We can obtain the desired resurt by taking the expression (4.1)< q^{n-k}.

can obtain the desired result by the expression (4.1) less than equal to the number of all possible cosets.

i.e.

$$q^{n-k} \geq 1+\frac{f(q-1)}{3}\left(2^{2(\beta+1)}-1\right).$$

The following theorem provides the suficient conditon required to exist a code that can locate the RK errors in a single sub-block.The famous bound, Varshamov-Gilbert-Sacks Bound (refer Theorem 16.4, [8]) will be used to prove this theorem. This bound provideds a technique to construct a PC matrix for codes. This theorem is verified by giving an example.

Theorem 4.2. The construction of a PC matrix is possible that ensures the existence of an $(n = fl, k)$ code ($l > 2\beta$) over *GF*(*q*) capable to locate the restricted key errors of length β or less if the follwing condition is satisfied.

$$q^{n-k} > 1+(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]\times$$
$$\left[1+(f-1)\left[\frac{2}{3}\left(2^{2\beta}-1\right)+\frac{(l-2\beta)}{3}\left(2^{(2\beta+1)}+1\right)+\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]\right].$$

Proof. The The existence of the codes capable to locate the RK errors in single sub-block is considered to be ensured if the construction of a PC matrix *H* for such codes is done. This task will be performed by using the VGS Bound. As per this bound, let us choose appropriate *n-k* tuples over *GF*(*q*) to make all the columns of the first $f-1$ sub-blocks together with the first $\rho-1$ columns of the f^{th} sub-block of *H.*

In accordance with condition (i), if column h_ρ is not a linear sum of the or fewer columns just preceding h_ρ, then the ρ^{th} column h_ρ of the PC matrix *H* can be added. i.e.,

$$h_\rho \neq u_1 h_{\rho-1}+u_2 h_{\rho-2}+u_3 h_{\rho-3}+.\cdots+u_\beta h_{\rho-\beta} \tag{4.2}$$

Where u_i,s are same field elements of *GF*(*q*). In expression (4.2), the calculation of the u_i coefficients is same as the calculation of the number of the restricted key errors occurring in last β position of a vector. This is given by

$$(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right] \tag{4.3}$$

Now, due the condition (ii) if column h_ρ is not a linear sum of the β or fewer columns just preceding h_ρ together with the linear combination of any set of $2\beta+1$ or less columns from any of $f-1$ sub-blocks, then the ρ^{th} column h_ρ of the PC matrix *H* can be added. i.e.,

$$\begin{aligned} h_\rho \neq\ & u_1 h_{\rho-1}+u_2 h_{\rho-2}+u_3 h_{\rho-3}+.\cdots+u_\beta h_{\rho-\beta} \\ & +v_1 h_1+v_2 h_2+v_3 h_3+.\cdots+v_{2\beta+1} h_{2\beta+1}, \end{aligned} \tag{4.4}$$

where u_i , $v_i \in GF(q)$. The number of u_i coefficients in expression (4.4) is same as in expression (4.3) u_i while the finding the number of coefficients v_i is similar to the finding the number of restricted key errors contained in a vector of length *l*. This is given by

$$(q-1)\left[\frac{2}{3}\left(2^{2\beta}-1\right)+\frac{(l-2\beta)}{3}\left(2^{(2\beta+1)}+1\right)+\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right].$$

Since there are $f-1$ such sub-blocks, therefore, due to the condition (ii), the number of linear sums is as:

$$(q-1)^2(f-1)\left[\frac{2}{3}\left(2^{2\beta}-1\right)+\frac{(l-2\beta)}{3}\left(2^{(2\beta+1)}+1\right)+\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]. \qquad (4.5)$$

Therefore, due to the expression (4.4) the number of all linear sums (including the vector of all zero components) that is not equal to h_ρ is

1+*Expr.* (4.3) + *Expr.* (4.5)

or

$$1+(q-1)\left[\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]\times$$
$$\left[1+(f-1)\left[\frac{2}{3}\left(2^{2\beta}-1\right)+\frac{(l-2\beta)}{3}\left(2^{(2\beta+1)}+1\right)+\frac{8}{9}\left(2^{2(\beta-1)}-1\right)+\frac{\beta+2}{3}\right]\right].$$

The required result will be obtained by putting this expression less than q^{n-k}.

This section is concluded by giving an example of a code that locates the RK errors of length upto β.

Example 4.3. Taking $q=3$, $\beta=2$, $l=10$ in Theorem 4.2, we get a ternary (20, 13) linear code and its parity check matrix is given by

$$\begin{bmatrix}
1&0&0&0&0&0&0&1&1&1&1&1&1&1&1&1&1&0&1&1\\
0&1&0&0&0&0&0&0&1&1&0&0&1&2&1&1&0&1&2&0\\
0&0&1&0&0&0&0&2&0&1&2&0&0&1&1&2&0&0&1&2\\
0&0&0&1&0&0&0&2&2&1&0&2&1&0&1&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&1&1&0&1&0&0&1&2&2&0&0\\
0&0&0&0&0&1&0&1&1&1&0&0&0&2&0&0&0&1&0&2\\
0&0&0&0&0&0&1&2&2&1&2&1&1&1&0&0&2&0&0&0
\end{bmatrix}$$

By preparing error patterns syndrome table, we can verify that all the syndromes of RK errors of length upto 2 occurring in different sub-blocks are non-zero and distinct. So, this is a ternar code is capable to locate the key errors of length upto 2.

5. REFERENCES:

[1] Kindra, B., Kumar, M. and Kumar, S: *Repeated restricted bursts error correcting linear codes Over GF(q):q>2.*Malaya Journal of Matematik, **9**(1), 917-921, (2021).

[2] Berardi, L., Dass, B.K. and Verma, R.: *On 2-repeated burst error detecting linear codes*. Journal of Statistical Theory and Practices, **3**(2), 381-391 (2009).

[3] Chien, R.T. and Tang, D.T.: , On definition of a burst, IBM J. Res. Dev., 9(4), 292-293, (1965).

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

[5] Das, P.K., Kumar, S., *Location and weight distribution of key errors*, Matematicki Vesnik, **73**(1), 43--54, (2021).

[6] Das, P.K., Kumar, S., *Blockwise and low density key error correcting codes*, International Journal of Mathematical, Engineering and Management Sciences, **5**(6), 1234-1248, (2020).

[7] B.K. Dass and S. Madan: Blockwise repeated burst error correcting linear codes, Ratio Mathematica-Journal of Applied Mathematics, **20**, 97--126 (2010).

[8] Dass, B.K. and Verma, R.: *Repeated burst error correcting linear codes*, Asian-European. Journal of Mathematics, **1**(3), 303—335, (2008).

[9] Fire, P.: A class of multiple-error -correction binary codes for non-independent errors, Sylvania Report RSL-E-2, Sylvania Reconnaissance Systems Laboratory, Mountain View, California. (1959).

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

[11] Peterson, W.W. and Weldon (Jr.), E.J., Error-correcting codes, 2nd edition, MIT Press, Mass. (1972).

[12] Sacks, G.E.: Multiple error correction by means of parity-checks, IRE Trans. Inform. Theory, IT-4, 145-147 (1958).

[13] V. Tyagi, and Tarun Lata, *Restricted 2- burst correctingnon-binary optimal codes*, Journal of Combinatorics and System Sciences, **42**(1-4), 145–154 (2017).

[14] Wolf, J.K. and Elspas, B. *Error-locating codes: a new concept in error control*, IEEE Trans. Inform. Theory, **IT-9**, 20-28, (1963).

[15] Wyner, A.D., (1963), Low density burst correcting codes, IEEE Trans. Inform. Theory, **9**(2), pp. 124.