Restricted Key Errors Correcting Linear Codes

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

[1]Department of Mathematics, Shyam Lal College, University of Delhi-110032, India.
[1]skumarmath@shyamlal.du.ac.in
[2*]Department of Mathematics, PGDAV (E) College, University of Delhi-110065, India.
[2*]haripratap@pgdave.du.ac.in
[3]Department of Mathematics, Motilal Nehru College, University of Delhi-110021, India
[3]sunit@mln.du.ac.in
[4]Discipline of Statistics, Indira Gandhi National Open University, Delhi-110068, India.
[4]gajrajsingh@ignou.ac.in
[5]Department of Mathematics, Deshbandhu College, University of Delhi, India.
[5]manojccs@gmail.com
Corresponding author: - Hari Pratap

Received: 21.06.2024 Revised: 19.08.2024 Accepted: 07.09.2024

ABSTRACT

This correspondence represents the codes having the nature of correcting the restricted key errors occurring in the whole code length. A comparison is also established among the restricted key errors and ordinary key errors.

Keywords: Restricted Key Errors (RK Errors), Detection, Correction, Parity Check Matrix (PCM), Error Patterns, Syndromes.
Subject Classification [2010**]:** 94B05, 94B65

1. INTRODUCTION

The communication channels can be divided into two categories. First of them consists those channels which transmit the information through the wires and the second has the wireless communication channels. In both the cases the transmission may be effected due the internal or external factors. For example, Due to the damaged wires a telephone user may face voice break problem. In the case wireless communication channels transmission can be disrupted due the lightning in the bad weather. Such type of disturbances during the transmission are said to be noises or errors. There are many types of errors such as random errors [9], burst errors [8], solid burst errors [12], repeated burst errors [6, 7], restricted solid burst errors [13], restricted repeated burst errors [1] etc.

Sharma and Gaur in their paper [11] pointed out a different type of error while dealing with typing error on a computer key board. Later, this error was named as ``*key error*'' by Das [3]. 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 intended key, then a word with no or different meaning appears. In this case, a key error is created. The definition of a key error is given by Das [3] as "*An i-key error of length λ $(i = 1, 2,\ldots, n)$ is an n-tuple such that the i^{th} component is non-zero* *and all other nonzero components are confined upto λ consecutive positions (if exist) immediately preceding and succeeding the i^{th} component.*" The vectors, $(\underset{\substack{entry\\error}}{2}\,01000)$, $(032\,\underset{\substack{entry\\error}}{3}\,10)$, $(21\,\underset{\substack{entry\\error}}{3}\,3100)$ etc. are examples of key errors of length 2 over *GF*(4). These key errors are studied in the papers [3-5].

A restricted key error of given length is obtained by imposing a restriction on the field elements occupying the places in a key error. The definition of a restricted key error is given in the paper [2], as:

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 λ 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.

In this research paper [2], the authors obtained the key error detecting and correcting codes. In the following section, number of all vectors are determined in the different part of a vector of length *n*.

2. RK ERROS OCCURRING IN A VECTOR

The RK errors of length λ or less lying in a vector of length n can be figure out from the key errors in Theorem 2.1 of [4] by multiplying $(q-1)$ to the number of key errors obtained in binary case for each corresponding case . A vector of length n can be divided into three parts to find the exact number of RK errors.

(a).[2] In this case that the entry error i fluctuates between the first and the λ^{th} positions, the total number of RK errors is determined by

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

(b). [2] When i fluctuates between the $(\lambda+1)^{th}$ place and the $(n-\lambda)^{th}$ positions, the total number of RK errors is as

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

(c). [2] If i fluctuate between the $(n-\lambda+1)^{th}$ place and the n^{th} position, the total number of RK errors is as

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

The sum of RK errors of length up to λ in an *n* tuple is therefore,

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

i.e.

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

3. CORRECTION OF RESTRICTED KEY ERRORS

In this section we provide the bounds for the codes capable to correct the RK errors. For these codes, The syndromes corresponding to the RK errors satisfy the conditions given below.

(i) The syndromes corresponding to the RK errors in the whole code length must be different from zero vector.

(ii) The syndromes corresponding to the RK errors must be different from the syndromes corresponding to the other RK errors occurring in the whole code length.

Theorem 3.1. *To correct the restricted key errors of length λ occurring in the whole code length of an (n,k) code $(n>4\lambda)$ over GF(q) with k information digits, the following condition must be satisfied.*

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

Proof. The required result can be proved same as the Theorem 3.1 of [2] by caculating the the number of all the restricted key errors occurring in the whole code length and are to be corrected.

The expression (2.4) represents the number of all restricted key erors. We can get the required result by puting this number less than or equal to the total number of all possible cosets. i.e.

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

The following theorem provides the suficient conditon required to exist a code that can correct the RK errors occurring in the whole code length. 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 correct the restricted key errors of length λ or less if the follwing condition is satisfied.*

$$q^{n-k} > 1+(q-1)\left[\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right]\times$$
$$\left[1+(q-1)\left[\frac{2}{3}\left(2^{2\lambda}-1\right)+\frac{(n-4\lambda)}{3}\left(2^{(2\lambda+1)}+1\right)+\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right]\right].$$

Proof. To ensure the existence of an (*n*, *k*) code over *GF*(*q*) capable to correct the restricted key errors of length λ or less we will construct a parity check matrix for the code by folowing the same technique used in Theorem 4.16 [10]

Let by suitabale selection of *n-k* tuples over *GF*(*q*), we have put first $\rho-1$ columns of *H*.

According to the condition (i),

i.e.

$$h_\rho \neq u_1 h_{\rho-1}+u_2 h_{\rho-2}+u_3 h_{\rho-3}+.\cdots+u_\lambda h_{\rho-\lambda} \quad (3.1)$$

Where u_i's are same field elemnets of $GF(q)$. In expression (3.1), the calculation of the u_i coefficients is same as the calculation of the number of the the ρ^{th} column h_ρ of the PC matrix H can be added if column h_ρ is not the linear combination of the λ or fewer columns just preceding h_ρ .restricted key errors occurring in last ρ possition of a vector. Which is given by

$$(q-1)\left[\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right] \tag{3.2}$$

Now , according to the condition (ii), the ρ^{th} column h_ρ of the PC matrix H can be added if column h_ρ is not the linear combination of the λ or fewer columns just preceding h_ρ together with the linear combination of any set of $2\lambda+1$ or less columns from the first $\rho-2\lambda$ columns.
i.e.

$$\begin{aligned} h_\rho &\neq u_1h_{\rho-1}+u_2h_{\rho-2}+u_3h_{\rho-3}+.\cdots+u_\lambda h_{\rho-\lambda} \\ &+v_1h_1+v_2h_2+v_3h_3+.\cdots+v_{2\lambda+1}h_{2\lambda+1} \end{aligned} \tag{3.3}$$

Where u_i , $v_i \in GF(q)$. The number of u_i cofficients in expression (3.3) is same as in expression (3.2) while the calculation of the number of coefficients v_i ,s is similar to the calculation of the number of the restricted key errors lying in a vector of length $\rho-2\lambda$ that is in a sub-block. This is given by

$$(q-1)^2\left[\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right]\times\left[\frac{2}{3}\left(2^{2\lambda}-1\right)+\frac{(\rho-4\lambda)}{3}\left(2^{(2\lambda+1)}+1\right)+\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right]. \tag{3.4}$$

Therfore, due to the expression (3.3), the total number of l.c. (including the vector of all zero components) that is not equal to h_ρ is given by

1+*Expr*. (3.2) + *Expr*. (3.4)

Since there are q^{n-k} cosets, Therefore

$$q^{n-k} > 1+\text{Expr.}(3.2)+\text{Expr.}(3.4)$$

or

$$q^{n-k} > 1+(q-1)\left[\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right]\times$$
$$\left[1+(q-1)\left[\frac{2}{3}\left(2^{2\lambda}-1\right)+\frac{(\rho-4\lambda)}{3}\left(2^{(2\lambda+1)}+1\right)+\frac{8}{9}\left(2^{2(\lambda-1)}-1\right)+\frac{\lambda+2}{3}\right]\right].$$

The required result will be obtained by replacing ρ by n this expression.

We conclude this section by giving an example of the code that locates the RK errors of length upto λ .

Example3.1. Taking $q=3, \lambda=2$, $n=22$ in Theorem 3.2, we get a ternary (22, 11) linear code and its parity check matrix is given by

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

By preparing error patterns syndrome table, we can verify that all the syndromes of RK errors of length upto 2 occurring in whole code legth are non-zero and distinct. So, this ternary code is capable to correct the restricted key errors of length upto 2.

4. COMPARISON AMONG THE PARITY CHECK DIGITS

Table 4.1: Comparison on necessary number of check symbols

S. N.	λ	n	n-k in Theorem 2.1 [3]	n-k in Theorem 3.1
1	2	7	6	5
2	3	9	8	6
3	4	11	10	7
4	5	13	12	8
5	6	15	14	10

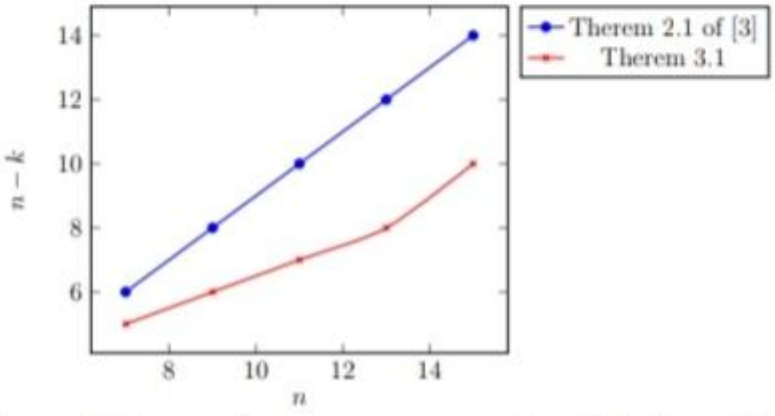

Figure 4.1: Comparison on necessary number of check symbols

The Figure 4.1 obtained form the Table 4.1 compares the redundancy of the codes given by the Theorem 2.1 in paper [3] with the redundancy of our codes given by the Theorem 3.1.

It can be observed that the codes obtained in this paper carry less PC digits in comparison of the PC digits required for the codes obtained in the Theorem 2.2 in paper [3]. In other words it can be said that the codes developed in this pape are more efficient.

Now, we will discuss the comparison of PC digits of ordinary key errors correcting codes and restricted key error correcting codes

Table 4.2: Comparison on sufficient number of check symbols

S. N.	λ	n	n-k in Theorem 2.1 [3]	n-k in Theorem 3.2
1	2	11	9	7
2	3	15	13	9
3	4	20	18	12
4	5	24	22	15
5	6	30	26	18

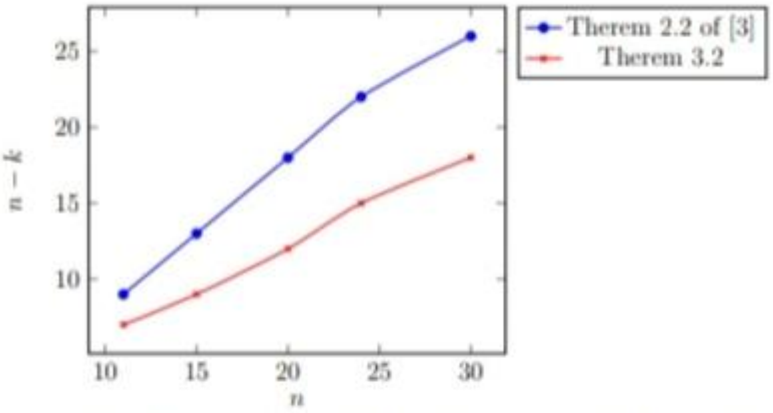

Figure 4.2: Comparison on sufficient number of check symbols

The Figure 4.2 obtained from the Table 4.2 compares the redundancy of the codes given by the Theorem 2.2 in paper [3] with the redundancy of our codes given by the Theorem 3.2.

It can be observed that the codes obtained in this paper carry less PC digits in comparison of the PC digits required for the codes obtained in the Theorem 2.2 in paper [3]. In other words it can be said that the codes developed in this paper are more efficient.

5. CONCLUSION

In this communication, we have derived the lower and upper bounds for the number of PC digits required for the codes having the capabilty of correction of the restricted key errors and verified these codes by providing one example of PCM. It will be for further research if the repeated restricted key errors and the codes that can deal with these errors can be obtained.

Acknowledgement: We are very thankful to Prof. Pankaj Kumar Das for his critical observation about the key errors and giving the method to calculate the number of key errors occuring in a vector in his paper entitled "Codes correcting Key Errors".

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] Kumar, S., Pratap, H., Kumar, M., Singh, G., Agrawal, N., Detection and Location of Restricted Key Errors, accepted for publication in Journal of Computational Analysis and Applications.

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

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

[5] 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).

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

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

[8] 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).

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

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

[11] Sharma, B.D. and Gaur, A. \textit{Codes correcting limited patterns of random errors using S-K metric}, Cybernetics and Information Technologies, 13(1), 34-45, 2013.

[12] Schillinger, A.G., A class of solid burst error correcting codes, Polytechnic Institute of Brooklyn , N.Y.,Research Rept. PIBMRI, April, pp. 1223-64, 1964.

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