Journal of Algebra and Applied Mathematics
Vol. 21 (2023), No.1, pp.17-34
ISSN: 2319-7234
© SAS International Publications
URL : www.sasip.net

Five errors correcting (73, 61, 12) quadratic residue code over ternary field

P. Shakilabanu and T. Suganthi

Abstract. This paper investigates the error-correcting performance of (73,61,12) quadratic residue code over a ternary field. A technique used to determine unknown syndromes of binary quadratic residue code is applied to the non-binary case to decode the ternary quadratic residue code of length 73. Furthermore, known and unknown syndromes are produced using the error-locator polynomial.

AMS Subject Classification (2020): 94B15, 94B35, 94B60

Keywords: Cyclic codes, idempotent generators, quadratic residue codes, error locators and syndromes

1. Introduction

The well-known quadratic residue (QR) codes were introduced by Prange [12] in 1958.These codes are typically half-rate cyclic codes with powerful error correction capabilities. Over the last few decades, many decoding methods for binary QR codes 11 have been given advanced. There are a total of 11 binary QR codes with code lengths of less than 100: 7, 17, 23, 31, 41, 47, 71, 73, 79, 89, and 97. The corresponding algebraic decoding methods for these QR codes are known as the Sylvester resultant [5] or Grobner basis methods [8]. These methods can be used to solve Newton's identities [6], which are high-degree nonlinear and multivariate equations. However, the calculations of identities require significant computational effort, especially when the weight of the corresponding error pattern becomes large.Therefore,these methods are only suitable for relatively short QR codes. The Berlekamp-Massey algorithm [4] was used to decode the QR codes with code lengths of 71, 79 and 97 in [1].

In previous decades, the Sylvester resultant [5], [11], or Grobner basis approaches [2] were the most extensively used methods for deciphering binary QR codes. These approaches may be used to solve Newton identities, which are nonlinear and multivariate equations with a high degree of complexity. However, calculating identities requires a significant level of computing cost, particularly when the weight of the encountered mistake pattern is considerable. Furthermore, because various QR codes utilise different sets of circumstances to generate error sites, enumerating all situations would be impractical for hardware implementation. Although the authors of [3] created an algebraic decoding strategy based on Newton identities for decoding the (73, 37, 13) QR code, the simulation results were not supplied due to extremely complicated computations. Later, the authors [4] used the well-known Berlekamp-Massey (BM) method to decode QR codes. Once the necessary consecutive symptoms are collected, it is quite efficient.

Lin & Wang et al. [9], [21] enhanced the decoding performance of the QR code of length 89 even more by swiftly detecting unknown syndromes. However, the circumstances corresponding to mistake patterns with varying weights have yet to be discovered. Li et al. [7] suggested an improved decoding technique for the (73, 37, 13) QR code. It was built on the [15] hybrid unknown syndrome calculation (HUSC) method and the modified inverse-free BM algorithm. Furthermore, by adding more linear constraints created by redundant parity checks (RPC), the performance of Linear Programming (LP) decoding can be increased [13], [14], [19] and [20]. Although the majority of the LP decoding algorithms were designed to decode low-density parity-check (LDPC) codes, they also performed admirably when used to decode Bose Chaudhuri Hocquenghem (BCH) codes, Golay codes, the (89, 45, 17), and the (73, 37, 13) QR codes, as shown in [4], [14], [16], and [20]. One of the intriguing experimental results in [22] is that the (73, 37, 13) QR code performed better than the (89, 45, 17) QR code [20] and [22] with much less multiplications and adds when LP decoding was used, despite the latter having a greater minimum distance.

Algebraic decoding of binary codes can be performed using the Peterson or Berlekamp-Massey algorithm once certain unknown syndromes are determined. The method for determining unknown syndromes was first used by Ruhua et al. [17] to decode the binary QR code of length 47 and then to decode several other binary QR codes. Interlando [6] decoded the ternary quadratic residue code of length 23. This ternary QR code can only correct up to four errors. To the best of our knowledge, there has been no ternary QR code study that corrected more than four errors. This article examines the ability to correct five errors of ternary QR codes with a code length of 73. We used the binary decoding method to detect and correct five errors over $F_3^{(12)}$ using known and unknown syndromes. The generator of this QR code is an irreducible generator polynomial [18].

The main idea is to identify certain unknown syndromes to restore the linearity of Newton identities. The main focus is on the calculation of the error location polynomial. Error-values are found from the evaluator polynomial [10, p.246] as soon as the error locations are determined.

In this paper, Section 1 contains the introduction and Section 2 contains the background of ternary QR codes. Section 3 presented algorithm to determine the unknown syndromes. The determination of unknown syndrome S_5 is calculated in Section 4. In Section 5, calculation of $\sigma(x)$ for the ternary (73,37,16) QR code and also Section 6 contains the applications of the proposed algorithm. Finally, Section 7 contains the conclusion of the paper.

2. Background of ternary QR codes

A ternary QR code (n,k,d) or (n,(n+1)/2,d) with minimum distance d is defined algebraically as a multiple of its generator polynomial over GF(3),where k=(n+1)/2 is the message length and n is the code length. Let n=12r±1 be a prime number,where r is a positive integer and m is the smallest positive integer such that 3^m≡1(modn).

As usual, let E= GF(3^{12}) be the defining field of the (73,61,12) QR code,First compute the set of quadratic residues modulo 73, Q_{73}, as follows:

$$
\begin{aligned}
Q_{73} &= \{i/i \equiv j^2 \bmod 73 \;\text{ for }\; 1 \le j \le 72\} \\
&= \{1,2,3,4,6,8,9,12,16,18,19,23,24,25,27,32,35,36,37,38,41,46,48, \\
&\quad 49,50,54,55,57,61,64,65,67,69,70,71,72\}. \qquad (1)
\end{aligned}
$$

If α is a primitive element of E, then $\beta = \alpha^{7280}$ is a primitive 73^{rd} root of unity in E. The QR code of length $n = 73$ is a cyclic code with a idempotent polynomial $E(x)$ is generated by:

$$E(x) = 1 + e_2(x), \qquad (2)$$

where $e_2(x) = \sum_{i \in N} x^i$, and N is the set of non-residues modulo 73.

Denote the set $\{0\} \cup Q_{73}$ by Z and define the polynomial $g(x) \in f_3(x)$ is given by,

$$
\begin{aligned}
g(x) &= \prod_{1 \in z}^{2} \{(x - \beta^i)\} \\
&= x^{12} + 2x^{11} + x^{10} + x^9 + x^8 + x^7 + x^5 + x^4 + x^3 + x^2 \\
&\quad + 2x + 1. \qquad (3)
\end{aligned}
$$

A ternary vector c=$(c\dot{}0, c\dot{}1, c\dot{}2, ...c\dot{}72)$ is a codeword if and only if its associated polynomial $c(x) = c_0 + c_1x + \cdots + c_{72}x^{72}$ is a multiple of $g(x)$. If $r = (r_0, r_1, \cdots r_{72})$ is a received vector, then its associated polynomial $r(x) = r_0 + r_1x + \cdots + r_{72}x^{72}$ can be expressed as a sum of the transmitted code polynomial $c(x)$ and error polynomial $e(x) = e_0 + e_1x + \cdots + e_{72}x^{72}$.

The set of known syndromes is obtained by evaluating r(x) at the roots of $g(x)$, namely

$$S_i = c(\beta^i) + e(\beta^i) = e(\beta^i) \text{ for } i \in Q_{73}. \tag{4}$$

If v errors occur in the received polynomial then the error polynomial has v non-zero terms, namely

$$e(x) = x^{r_1} + x^{r_2} + \cdots + x^{r_v}, \tag{5}$$

where $0 \leq r_1 < r_2 < \cdots < r_v \leq 72$ for $i \in Q_{73}$, and the i-th syndrome S$_i$ is given by

$$S_i = (\beta^{r_1})^i + (\beta^{r_2})^i + \cdots (\beta^{r_v})^i + = (x_1)^i + (x_2)^i + \cdots (x_v)^i \tag{6}$$

where $x_j = \beta^{r_j}, 1 \leq j \leq v$, are called error locators.

For the (73,61,12) QR code,one has the following equalities among the known syndromes: $S_3 = S_1^3, S_8 = S_1^{3^4}, S_9 = S_1^{3^2}, S_{24} = S_1^{3^5}, S_{27} = S_1^{3^3}, S_{46} = S_1^{3^9}, S_{49} = S_1^{3^{11}}, S_{64} = S_1^{3^8}, S_{65} = S_1^{3^{10}}, S_{70} = S_1^{3^7}, S_{72} = S_1^{3^6}$.

To determine the error locators x$_i$, define the error-locator polynomial $\sigma(x)$ as follows:

$$\sigma(x) = x^v + \sum_{j=0}^{v-1} \sigma_{v-j}x^j, \tag{7}$$

where the ${\sigma_i}^s$ are the elementary symmetric functions, which are related to the syndromes via Newton's identities [6, PP.244-246]

$$S_k + \sum_{j=1}^{v} S_j\sigma_{k-j} = 0, \text{ for } k \in Z \tag{8}$$

which can be solved efficiently when there is a sufficient number of consecutive known syndromes. For the (73,61,12) code, the minimal distance is 12.This can correct upto 5 errors; however, the only syndromes that can be determined directly from $r(x)$ are $S_1, S_2, S_3, S_4, S_6, S_8$ and S_9. But S_5, S_7 and S_{10} are cannot be obtained by evaluating $r(x)$ at the roots of $g(x)$.

3. Algorithm to determine the unknown syndromes

Step 1. Let $I = \{i_1, i_2, \cdots i_{v+1}\} \subseteq \{0, 1, 2, ...72\}$ consisting of v+1 distinct elements.

Step 2. Define a matrix $X(I)$ of size $(v+1)\times v$ as follows:

$$X(I) = \begin{pmatrix} z_1^{i_1} & z_2^{i_1} \cdots & z_v^{i_1} & \\ z_1^{i_2} & z_2^{i_2} & \cdots & z_v^{i_2} \\ . & . & . & \\ . & . & . & \\ z_1^{i_v} & z_2^{i_v} & \cdots & z_v^{i_v} \\ z_1^{i_{v+1}} & z_2^{i_{v+1}} & \cdots & z_v^{i_{v+1}} \end{pmatrix}$$

Step 3. Let $J = \{j_1, j_2, \cdots j_{v+1}\}$ be another $(v+1)$ subset of $\{0, 1, 2, ...72\}$ and define a matrix $S(I, J)$ such that

$$S(I, J) = X(I) \times X(J)^T. \tag{9}$$

Theorem 1 [3]. *The (v+1)×(v+1) matrix $S(I, J)$ in (8) has the form*

$$S(I, J) = \begin{pmatrix} S_{i_1+j_1} & S_{i_1+j_2} & \cdots & S_{i_1+j_{v+1}} \\ S_{i_2+j_1} & S_{i_2+j_2} & \cdots & S_{i_2+j_{v+1}} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ S_{i_{v+1}+j_1} & S_{i_{v+1}+j_2} & \cdots & S_{i_{v+1}+j_{v+1}} \end{pmatrix}.$$

where the summation of the sub-induces of s_i are modulo 72. Moreover, the determinant of $S(I, J)$ is zero, i.e., $det(S(I, J))$ =0.

Theorem 2 [4]. *If among the entries of $S(I, J)$, there is only one unknown syndrome, say S_r, then S_r can be expressed as the quotient of two determinants of matrices obtained from $S(I, J)$. If S_r appears in the $(i, j)^{th}$ position of $S(I, J)$, then*

$$S_r = det(\Delta_0)/det(\Delta). \tag{10}$$

where Δ_0 is the $(v+1)' \times (v+1)$ matrix that is identical to $S(I, J)$ except with the $(i, j)^{th}$ equal to 0 instead of S_r, and Δ is the $v' \times v$ submatrix of $S(I, J)$, obtained by deleting the i^{th} row and j^{th} column of $S(I, J)$.

4. Determination of unknown syndrome $\mathbf{S}_5$

The six possible Cases 0 to 5 are disscussed separately,where the case number indicates the number of errors for that case.For each case, the two subsets I and J required in Theorem 1 to determine the primary unknown syndrome S_5 are explicitly listed. The other unknown syndromes S_7, S_{10} can be expressed in terms of S_5 as follows:

$$S_7 = S_5^{16}, S_{10} = S_5^2.$$

Moreover the attachment of a superscript to "S_5" to obtain the notation "$S_5^{(v)}$" indicates that it is valid for the v-error case only.

Case 0. (0 error)

In this case, error $v = 0$.

The unknown syndrome is $S_5^{(0)} = 0$.

Case 1. (1 error)

For v =1, let us choose $I_1 = \{2, 3\}$ and $J_1 = \{2, 6\}$.

Then, by Theorem 1, one obtains the matrix $S(I_1, J_1)$ of size 2×2,

$$S(I_1, J_1) = \begin{pmatrix} S_4 & S_8 \\ S_5^{(1)} & S_9 \end{pmatrix}.$$

where $S_0 = 1$. Thus,one can solve for the unknown syndrome $S_5^{(1)}$ for the 1-error case as follows:

$$S_5^{(1)} = det(\Delta_0)/det(\Delta)$$

where

$$\Delta = S_8 \text{ and } \Delta_0 = \begin{pmatrix} S_4 & S_8 \\ 0 & S_9 \end{pmatrix}$$

This is a trivial case. By definition of a syndrome for the 1-error case, $S_5^{(1)} = (Z_1)^5 = S_1^5$.

Case 2. (2 errors)

For v =2, let us choose $I_2 = \{4, 5, 8\}$ and $J_2 = \{1, 4, 19\}$. Then, by Theorem 1, one obtains the matrix $S(I_2, J_2)$ of size 3×3,

$$S(I_2, J_2) = \begin{pmatrix} S_5^{(2)} & S_8 & S_{23} \\ S_6 & S_9 & S_{24} \\ S_9 & S_{12} & S_{27} \end{pmatrix}.$$

where $S_0 = 0$. Thus, by Theorem 2, one can solve for the unknown syndrome $S_5^{(2)}$ for 2-error case using

$$S_5^{(2)} = det(\Delta_0)/det(\Delta).$$

where

$$\Delta = \begin{pmatrix} S_9 & S_{24} \\ S_{12} & S_{27} \end{pmatrix}$$

and

$$\Delta_0 = \begin{pmatrix} 0 & S_8 & S_{23} \\ S_6 & S_9 & S_{24} \\ S_9 & S_{12} & S_{27} \end{pmatrix}.$$

Case 3. (3 errors)

For v=3, let us choose $I_3 = \{0, 2, 4, 5\}$ and $J_3 = \{1, 4, 67, 69\}$. Then, by Theorem 1, one obtains the matrix $S(I_3, J_3)$ of size 4×4,

$$S(I_3, J_3) = \begin{pmatrix} S_1 & S_4 & S_{67} & S_{69} \\ S_3 & S_6 & S_{69} & S_{71} \\ S_5^{(3)} & S_8 & S_{71} & S_0 \\ S_6 & S_9 & S_{72} & S_0 \end{pmatrix}.$$

where $S_0 = 1$. Thus, by Theorem 2, one can solve for the unknown syndrome $S_5^{(3)}$ for 3-error case using

$$S_5^{(3)} = det(\Delta_0)/det(\Delta)$$

where

$$\Delta = \begin{pmatrix} S_4 & S_{67} & S_{69} \\ S_6 & S_{69} & S_{71} \\ S_9 & S_{72} & S_1 \end{pmatrix} . \text{ and } \Delta_0 = \begin{pmatrix} S_1 & S_4 & S_{67} & S_{69} \\ S_3 & S_6 & S_{69} & S_{71} \\ 0 & S_8 & S_{71} & S_0 \\ S_6 & S_9 & S_{72} & S_1 \end{pmatrix} .$$

Case 4. (4 errors)

For v=4, let us choose $I_4 = \{2, 3, 4, 5, 6\}$ and $J_4 = \{67, 69, 70, 71, 72\}$. Then by Theorem 1, one obtains the matrix $S(I_4, J_4)$ of size 5×5,

$$S(I_4, J_4) = \begin{pmatrix} S_{69} & S_{71} & S_{72} & S_0 & S_1 \\ S_{70} & S_{72} & S_0 & S_1 & S_2 \\ S_{71} & S_0 & S_1 & S_2 & S_3 \\ S_{72} & S_1 & S_2 & S_3 & S_4 \\ S_0 & S_2 & S_3 & S_4 & S_5^{(4)} \end{pmatrix} .$$

where S_0 =0. Thus, by Theorem 2, one can solve for the unknown syndrome $S_5^{(4)}$ for the 4-error case as follows:

$$S_5^{(4)} = det(\Delta_0)/det(\Delta).$$

where

$$\Delta = \begin{pmatrix} S_{69} & S_{71} & S_{72} & S_0 \\ S_{70} & S_{72} & S_0 & S_1 \\ S_{71} & S_0 & S_1 & S_2 \\ S_{72} & S_1 & S_2 & S_3 \end{pmatrix}$$

and

$$\Delta_0 = \begin{pmatrix} S_{69} & S_{71} & S_{72} & S_0 & S_1 \\ S_{70} & S_{72} & S_0 & S_1 & S_2 \\ S_{71} & S_0 & S_1 & S_2 & S_3 \\ S_{72} & S_1 & S_2 & S_3 & S_4 \\ S_0 & S_2 & S_3 & S_4 & S_5 \end{pmatrix} .$$

In the 5-error case,there does not exist a pair of subsets$I, J \subseteq \{0, 1, 2, ...72\}$ such that S_5 appears exactly once in the matrix $S(I, J)$. Therefore, slightly different approach from the previous algorithm is required to find the unknown syndrome S_5 for these cases.

Case 5. (5 errors)

For V =5, let us choose, $I_5 = \{0, 1, 2, 4, 8, 71\}, J_5 = \{0, 1, 2, 8, 69, 71\}$, $I'_5 = \{0, 1, 2, 3, 4, 5\}$ and $J'_5 = \{0, 1, 2, 3, 8, 72\}$

Form the matrices $S(I_5, J_5)$ and $S(I'_5, J'_5)$, by using Theorem 1,

$$S(I_5, J_5) = \begin{pmatrix} S_0 & S_1 & S_2 & S_8 & S_{69} & S_{71} \\ S_1 & S_2 & S_3 & S_9 & S_{70} & S_{72} \\ S_2 & S_3 & S_4 & \underline{S_{10}} & S_{71} & S_0 \\ S_4 & S_5 & S_6 & S_{12} & S_0 & S_2 \\ S_8 & S_9 & \underline{S_{10}} & S_{16} & S_4 & S_6 \\ S_{71} & S_{72} & S_0 & S_6 & S_{67} & S_{69} \end{pmatrix}$$

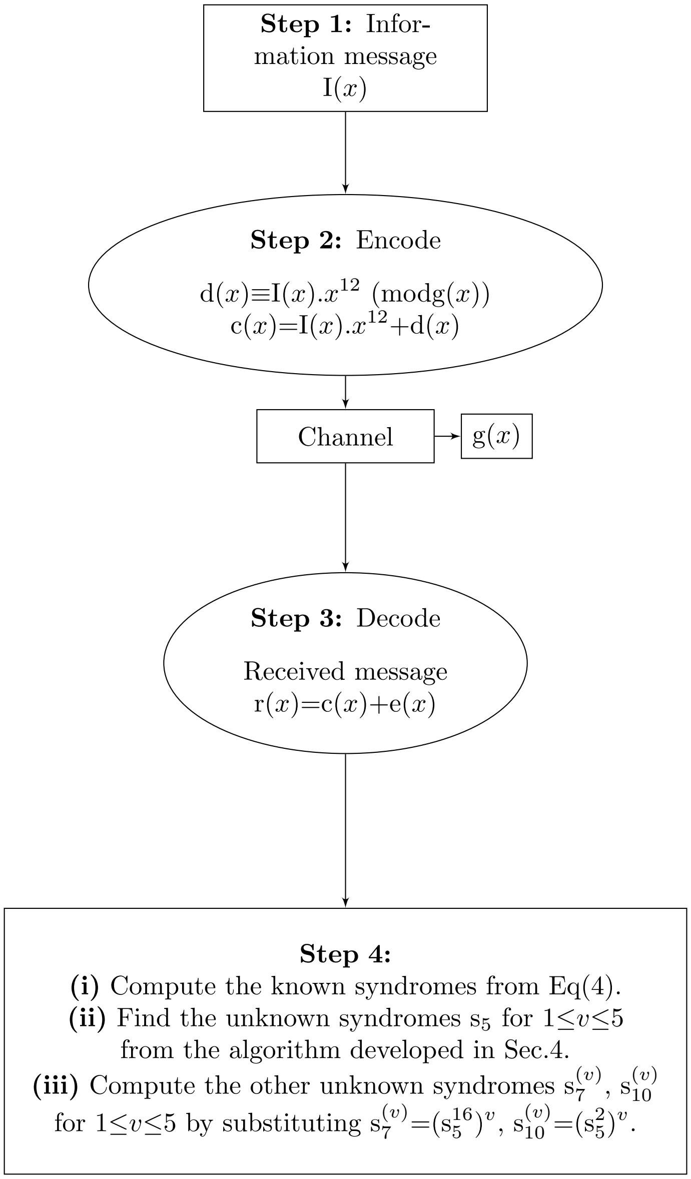
and

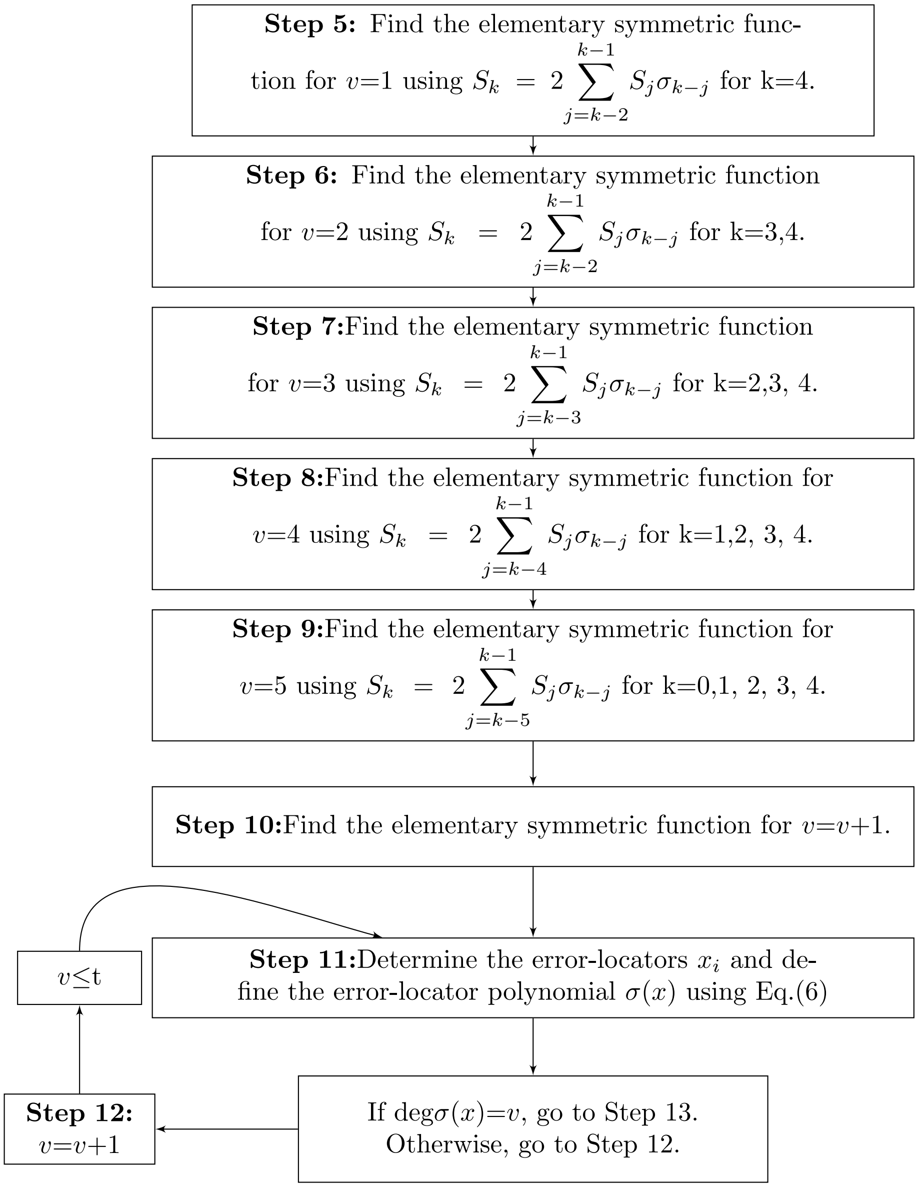
$$S(I'_5, J'_5) = \begin{pmatrix} S_0 & S_1 & S_2 & S_3 & S_8 & S_{72} \\ S_1 & S_2 & S_3 & S_4 & S_9 & S_0 \\ S_2 & S_3 & S_4 & \underline{S_5} & \underline{S_{10}} & S_1 \\ S_3 & S_4 & \underline{S_5} & S_6 & S_{11} & S_2 \\ S_4 & \underline{S_5} & S_6 & \underline{S_7} & S_{12} & S_3 \\ \underline{S_5} & S_6 & \underline{S_7} & S_8 & \underline{S_{13}} & S_4 \end{pmatrix}.$$

where $S_0 = 1$. All the entries in $S(_5, J_5)$ and $S(I'_5, J'_5)$ are known except for S_5, S_7, S_{10} and S_{13}. However, $S_7 = S_5^{16}, S_{10} = S_5^2$, and $S_{13} = S_5^{61}$. Therefore, $f_1 = detS(I_5, J_5)$ and $f_2 = detS(I'_5, J'_5)$ are polynomials in a single variable, namely S_5.

Let f =gcd(f$_1$,f$_2$). Thus,the required unknown syndrome S$_5$ for the 5-error case can be determined by solving $f(S_5)$ with the help of Theorem 2.

5. Calculation of $\sigma(x)$ for the ternary (73,37,16) QR code


Step 1: Information message I(x)
Step 2: Encode
d(x)≡I(x).x^{12} (modg(x))
c(x)=I(x).x^{12}+d(x)
Channel
g(x)
Step 3: Decode
Received message
r(x)=c(x)+e(x)
Step 4:
(i) Compute the known syndromes from Eq(4).
(ii) Find the unknown syndromes s_5 for $1 \leq v \leq 5$ from the algorithm developed in Sec.4.
(iii) Compute the other unknown syndromes $s_7^{(v)}$, $s_{10}^{(v)}$ for $1 \leq v \leq 5$ by substituting $s_7^{(v)}=(s_5^{16})^v$, $s_{10}^{(v)}=(s_5^2)^v$.



Step 5: Find the elementary symmetric function for v=1 using $S_k = 2\sum_{j=k-2}^{k-1} S_j\sigma_{k-j}$ for k=4.

Step 6: Find the elementary symmetric function for v=2 using $S_k = 2\sum_{j=k-2}^{k-1} S_j\sigma_{k-j}$ for k=3,4.

Step 7: Find the elementary symmetric function for v=3 using $S_k = 2\sum_{j=k-3}^{k-1} S_j\sigma_{k-j}$ for k=2,3, 4.

Step 8: Find the elementary symmetric function for v=4 using $S_k = 2\sum_{j=k-4}^{k-1} S_j\sigma_{k-j}$ for k=1,2, 3, 4.

Step 9: Find the elementary symmetric function for v=5 using $S_k = 2\sum_{j=k-5}^{k-1} S_j\sigma_{k-j}$ for k=0,1, 2, 3, 4.

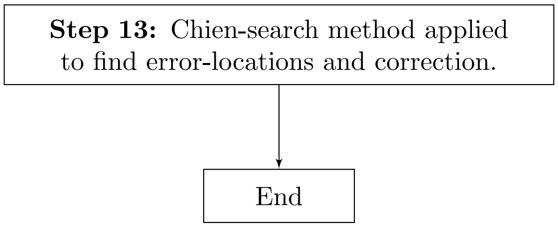
Step 10: Find the elementary symmetric function for v=v+1.

Step 11: Determine the error-locators x_i and define the error-locator polynomial $\sigma(x)$ using Eq.(6)

If deg$\sigma(x)$=v, go to Step 13. Otherwise, go to Step 12.

Step 12: v=v+1

v≤t


Step 13: Chien-search method applied to find error-locations and correction.
End

6. Application of the algorithm

To illustrate the above decoder for correcting errors, the algorithm is applied to the (13, 7, 5) QR code double-error correcting code over GF(3^3) generated by an irredcuible primitive polynomial $P(x) = x^3 + 2x + 1$ over GF(3). The details of this example are given here instead of the (73,61,12) case.

The set $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ consists of the quadratic residues modulo 13. Also, $\beta = \alpha^2$ is a primitive element of GF(3^3) satisfying $\alpha^3 + 2\alpha+1 = 0$. This code can correct 2 errors, and the single unknown syndrome is S_2.

For the cases of errors, the unknown syndrome $S_2^{(v)}$, $0 \le v \le 2$, is determined as follows:

For v=1,let $I_1 = \{0, 1\}$ and $J_1 = \{1, 9\}$. Then, by Theorem 1, one obtains the matrix $S(I_1, J_1)$ of size 2×2 ,

$$S(I_1, J_1) = \begin{pmatrix} S_0 & S_9 \\ S_2^{(1)} & S_9 \end{pmatrix}.$$

where $S_0 = 1$.

For v=2, let $I_2 = \{0, 1, 3\}$ and $J_2 = \{0, 1, 9\}$. Then, by Theorem 1,one obtains the matrix $S(I_2, J_2)$ of size 3×3,

$$S(I_2, J_2) = \begin{pmatrix} S_0 & S_1 & S_9 \\ S_1 & \underline{S_2^{(2)}} & S_{10} \\ S_3 & S_4 & S_0 \end{pmatrix}.$$

where $S_0 = 0$.

Assume the message polynomial $I(x) = x^3 + x^2 + 1$.

Multiplying the polynomial $I(x)$ by $g(x)$, one obtains the code polynomial $c(x) = I(x).x^6 + d(x) = x^9 + x^8 + x^6 + 2x^4 + 2x^3 + x^9 + x + 2$, where $d(x)$ is the remainder of $I(x).\ x^6$ divided by $g(x)$.

Two cases are discussed below.

Case 1. (1 error)

For the case of one error, assume the error polynomial is $e(x) = x^2$. Then the received polynomial is

$$\begin{aligned} r(x) &= c(x) + e(x) = x^9 + x^8 + x^6 + x^{24} + 2x^3 + x^2 + x + 2.S_i \\ &= (\beta^i)^9 + (\beta^i)^8 + (\beta^i)^6 + 2(\beta^i)^4 + 2(\beta^i)^3 + (\beta^i)^2 + \beta^i + 2 \text{ for } 1 \leq i \leq 4. \end{aligned}$$

That is $S_1 = \alpha^4$.

By (7), the single unknown syndrome for the 1-error case is $S_2^{(1)} = \alpha^8$. The error-locator polynomial $\sigma(x) = 1 + \alpha^{17}x$. The root of $\sigma(x)$ is $x_1 = \alpha^{-4} = \beta^{-2}$. Thus, the error polynomial is $e(x) = x^2$.

Case 2. (2 errors)

Assume that there are two errors in the received polynomial and the error polynomial $e(x) = x^3 + x^2$. Then the received polynomial

$$r(x) = c(x) + e(x) = x^9 + x^8 + x^6 + 2x^4 + x^2 + x + 2.$$

The known syndromes are,

$$S_i = r(\beta^i = (\beta^i)^9 + (\beta^i)^8 + (\beta^i)^6 + 2(\beta^i)^4 + (\beta^i)^2 + \beta^i + 2, \quad i = 1, 2, 3, 4,$$

i.e., $S_1 = \alpha^{25}, S_3 = \alpha^{23}, S_4 = \alpha^5, S_5 = 1$, and $S_6 = 1$.

By (7), the single unknown syndrome for the 2-error case is $S_2^{(2)} = \alpha^{12}$.

The error-locator polynomial is $\sigma(x) = \alpha^{10}x^2 + \alpha^{12}x + 1$. The roots of $\sigma(x)$ are $x_1 = \alpha^{-6} = \beta^{-3}$ and $x_2 = \alpha^{-4} = \beta^{-2}$. Thus,the error polynomial is $e(x) = x^3 + x^2$.

7. Conclusion

In this paper, we investigated the error-correcting performance of (73, 61, 12) quadratic residue code over a ternary field. The ternary field approach is more efficient when code is lengthy. A technique used to determine unknown syndromes of binary quadratic residue codes was applied to the non-binary case to decode the ternary quadratic residue code of length 73.

Acknowledgement. The authors would like to express their sincere gratitude to the referees for their valuable suggestions and comments which improved the paper.

References

[1] Y. Chang, T. Truong, I. Reed, H.Y. Cheng and C.D. Lee, *Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes*, IEEE Transactions on Communications, 51 (2003), 1463-1473.

[2] X. Chen, I.S. Reed, T. Helleseth, and T.K. Truong, *Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance*, IEEE Trans. Commun., 40 (1994), 1654-1661.

[3] X. Chen, I.S. Reed and T.K. Truong, *Decoding the (73, 37, 13) quadratic residue code*, IEE Proc. Comput. Dig. Tech., 141 (1994), 253-258.

[4] Y.H. Chen, T.K. Truong, Y. Chang, C.D. Lee, and S.H. Chen, *Algebraic Decoding of Quadratic Residue Codes Using Berlekamp-Massey*

Algorithm, Journal of Information Science and Engineering, 23 (2007), 127-145.

[5] M. Elia, *Algebraic decoding of the (23, 12, 7) Golay code Corresp.*, IEEE Transactions on Information Theory, 33 (1) (1987), 150-151.

[6] J.C. Interlando, *Decoding the Ternary (23, 11, 9) Quadratic Residue Code*, Research Letters in Communications, 107432 (2009).

[7] Y. Li, H. Liu, Q. Chen and T.K. Truong, *On decoding of the (73, 37, 13) quadratic residue Code*, IEEE Trans. Commun., (2014).

[8] T.C. Lin, H.P. Lee, H.C. Chang, S.I. Chu and T.K. Truong, *High speed decoding of the binary 47,24,11) quadratic residue code*, Information Sciences, 180 (2010), 4060-4068.

[9] T.C. Lin, W.K. Su, P.Y. Shih, and T.K. Truong, *Fast algebraic decoding of the (89, 45, 17) quadratic residue code*, IEEE Communication Letters, 15 (2011), 226-228.

[10] F.J. Macwilliams and N.J.A.Sloane, *The Theory of Error correcting Codes*, North- Holland Mathematical Library, 16 (1983).

[11] M. Miwa, T.Wadayama, and I. Takumi, *A cutting-plane method based on redundant rows for improving fractional distance*, IEEE J. Sel. Areas Commun., 27 (2009), 1005-1012.

[12] E. Prange, *Some cyclic error-correcting codes with simple decoding algorithms*, Air Force Cambridge Research Center TN, 156 (1958).

[13] J. Ravi, *A robust measure of pair wise distance estimation approach: RD-RANSAC*, International Journal of Statistics and Applied Mathematics, 2 (2017), 31-34.

[14] J. Ravi, *An Optimal Solution for Transportation problem-DFSD*, Journal of Computational Mathematica, 3 (2019), 43-51.

[15] I.S. Reed, X. Yin, and T.K. Truong, *Algebraic decoding of the (32, 16, 8) quadratic residue code*, IEEE Trans. Inf. Theory, 36 (1990), 876-880.

[16] I. S. Reed, T.K. Truong, X. Chen, and X. Yin, *The algebraic decoding of the (41, 21, 9) quadratic residue code*, IEEE Trans. Inf. Theory, 38 (1992), 974-985.

[17] H. Ruhua, I.S. Reed, T. Trieu-Kien and C. Xuemin, *Decoding the (47,24,11) quadratic residue code*, IEEE Transactions on Information Theory, 47 (2001), 1181-1186.

[18] P. Shakila Banu and T. Suganthi *Characterization of Quadratic Residue Codes over.* $\mathbb{Z}_{81}$, The International Journal Of Analytical And Experimental Modal Analysis, 11 (2019).

[19] M.H. Taghavi and P.H. Siegel, *Adaptive methods for linear programming decoding*, IEEE Trans. Inf. Theory, 54(2008), 5396-5410.

[20] A. Tanatmis, S. Ruzika, H.W. Hamacher, M. Punekar, F. Kienle and N. Wehn *A separation algorithm for improved LP-decoding of linear block codes*, IEEE Trans. Inform. Theory, 56 (2010), 3277-3289.

[21] L. Wang, Y. Li, T.K. Truong, and T.C. Lin, *On decoding of the (89, 45, 17) quadratic residue code*, IEEE Trans. Commun., 61 (2013), 832-841.

[22] X. Zhang and P.H. Siegel, *Adaptive Cut Generation Algorithm for Improved Linear Programming Decoding of Binary Linear Codes*, IEEE Trans. Inform. Theory, 58 (2012), 6581-6594.

Department of Mathematics
Vellalar College for Women
Thindal, Erode 638012
Tamilnadu
India
E-mail: shakimeeran10@gmail.com

Government Higher Secondary School
Vadugam, Rasipuram
Namakkal 637408
Tamilnadu
India
E-mail: : sugan1306thi@gmail.com

(*Received: October, 2022; Revised: December, 2022*)