Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2s (2024)

Eight Error Correction for (57,29,17) Quadratic Residue Code Over Binary Field

P. Shakila Banu[a], R.Shobana[b]
[a]Assistant Professor, Department of Mathematics, Vellalar College for Women,
Erode-638012, Tamilnadu, India
[b]Research Scholar, Department of Mathematics, Vellalar College for Women,
Erode-638012, Tamilnadu, India
E-Mail: [a] shakimeeran10@gmail.com, [b] shobanarj99@gmail.com

Article History:

Received: *26-03-2024*

Revised: *18-05-2024*

Accepted: *30-05-2024*

Abstract:

This paper introduces novel parameters and presents a method- ology for identifying the necessary syndrome indices required to compute the unknown syndromes within the context of the (57, 29, 17) quadratic residue code. By determining the resulting index sets, the unknown syndromes can be computed, subsequently leading to the derivation of the corresponding error-locator polynomial through the application of a de- coding algorithm.

Keywords: Algebraic Decoding, Quadratic residue code, Index set, Syndromes.

2020 subject classifications: 94B15, 94B35, 94B60.

1. Introduction

In 1958, Prange [11] pioneered the quadratic residue (QR) codes. Hamming addressed the issue of rectifying a single corrupted binary digit within any sequence of length n during the transmission of binary data over a noisy channel. Shapiro H.S. and Slotnick D.L. researched the equivalent problem for channels capable of corrupting a larger number of digits [13]. MacWilliams F.J. and Sloane N.J.A. comprehensively elucidated various forms of Error-Correcting Codes and decoding algorithms [7]. M. Elia achieved the decoding of the (23,12,7) Golay code by employing the algebraic decoding method for three-error-correcting BCH codes [2]. The researchers obtained the results of mathematical and analytical computations for multiple binary QR codes [17]. Additionally, they proposed a rapid method for identifying primitive polynomials over binary fields in [8]. The extended QR codes of lengths 32 and 48 exhibit non-linear binary pat- terns with significantly higher minimum weights were discussed in [10]. In the decoding process of the (47,24,11) QR code, the author devised two method- ologies to ascertain the nonlinear correlations between known and unknown syndromes, effectively rectifying five errors and diagnosing six errors [12]. The QR code was generated using the Truong et al decoding scheme with parameters (71,36,11), (79,40,15), and (97,49,15), accompanied by comprehensive computational modeling [18]. Furthermore, Chen et al. demonstrated a novel algebraic decoding technique for the (73,37,13) binary quadratic residue code in [1]. Lin et al. developed an amended decoding method specifically tailored for decoding the (48,24,12) extended binary QR code. This method enables the correction of up to six errors, leveraging the reliability-search algorithm pro- posed by Dubney et al. [16]. Utilizing Newton's identities, the coefficients of the error locator polynomial are determined, facilitating the creation of a decoding method aimed at reducing decoding time [15]. Additionally, various enhanced decoding techniques for 11 QR codes have been introduced through Grobner foundation techniques [5].

AH.P. Lee and H.C. Chang enhanced an algebraic decoding algorithm (ADA) to effectively decode up to five errors in binary systematic QR codes [3].

Additionally, the author proposed a hybrid algebraic decoding algorithm tailored to the specified parameters. In cases where the total number of errors v is five or fewer, the Laplace formula was utilized to derive the primary unknown syndromes. When v 6 and Gaussian elimination is utilized to figure out the unknown syndromes [6]. Truong et al. devised a method to compute unknown syndromes for the (73,37,13) QR code, with a focus on enhancing decoding performance using soft decisions. A comprehensive study was conducted to evaluate error-rate performance [4]. Furthermore, the author elaborated on numerous decoding algorithm techniques and error correction coding utilizing a mathematical approach [14]. In a separate study, Zhang et al. researched a hard decision (HD) strategy to correct up to five errors and decode the (47,24,11) QR code more efficiently [9]. Through simulation results, Zhang et al. demonstrated that the new HD algorithm reduces decoding complexity and conserves memory while maintaining the same error-rate performance [19].

In this paper, Section 1 contains the introduction and Section 2 carry preliminaries. In Section 3, the background of the QR code is discussed. The decoding algorithm for the (57,29,17) and the unknown syndromes are determined in Section 4. Section 5 contains the application of the algorithm and finally, the conclusion for this paper is given in Section 6.

2. Preliminaries

We will step over some fundamental definitions in this section that are related to our main concept.

Definition 2.1. [14] An (n, k) block code C is said to be $cyclic$ if it is linear and if every codeword $c = (c_0, c_1, \dots . c_{n-1})$ in C, its right cyclic shift $c' = (c_{n-1}, c_0, \dots , c_{n-2})$ is also in C.

Definition 2.2. [7] Let $GF(l)[x] \,/\, (x^p - 1)$ be a ring, where a prime number is p and the quadratic residue of p is $l, (x^p - 1) = (x - 1)q(x)n(x)$. Define the set of quadratic residues modulo p by Q_p, and the set of quadratic non-residues by N_p, Q, Q', N and $N'$are *quadratic residue codes*, which are cyclic codes (or ideals) of the ring with generator polynomials of $q(x), (x-1)q(x), n(x)$, $(x-1)n(x)$, so forth , where $q(x) = \prod_{i \in Q_p}(x - \alpha^i)$, $q(x) = \prod_{i \in Q_p}(x - \alpha^i)$ have coefficients from GF(l). In a field that contains GF(l), α represents a primitive p^{th} root of unity.

Definition 2.3. [14] An (n, k) cyclic code has a unique minimal monic polynomial $g(x)$, which is the generator of the ideal. This is called the *generator polynomial* for the code. Let the degree of g be $n - k$, $g(x) = g_0 + g_1 x + \cdots + g_{n-k} x^{n-k}$.

Definition 2.4. [14] An *irreducible polynomial* $p(x) \in GF(p)[x]$ of degree m is said to be primitive if the smallest positive integers n for which $p(x)$ divides $x^n - 1$ is $n = p^m - 1$.

Definition 2.5. [14] A sequence generated by a connection polynomial $g(x)$ of degree n is said to be a *maximal length* sequence if the period of the sequence is $2^n - 1$.

Definition 2.6. [14] A connection polynomial which produces a maximal-length sequence is a *primitive polynomial*.

3. Non-Binary (57,29,17) QR Code

The (*n*, *k*, *d*) parameters provide essential information about the capabilities and performance of error-correcting codes, guiding their design, implementation, and usage in various communication and storage systems. Let $\left(n, \frac{n+1}{2}, d\right)$ represent a binary QR code with generator polynomial $g(x)$ over $GF(2)$. The code length n, should be a prime number of the form $n = 8l \pm 1$, where m is the smallest positive integer such that n divides $2^m - 1$ and 1 is an arbitrary positive integer. The set Q of quadratic residue modulo n is the set of nonzero squares modulo n that is,

$$Q_n = \{j | j \equiv x^2 \, mod\, n,\ 1 \leq x \leq n-1\} \qquad (1)$$

For the binary (57, 29, 17) QR code, the components of codeword are in finite field $GF\,(2^{28})$ and its quadratic residue set is

$$Q_{57} = \{1,4,6,7,9,11,16,19,21,24,25,28,30,31,36,39,41,42,43,45,49,51,54,55\} \qquad (2)$$

A root of the primitive polynomial $x^{28} + x^3 + 1$ should be $\alpha \in GF(2^{28})$ [1]. The multiplicative group of nonzero elements in the finite field $GF(2^{28})$ is thus generated by α. It follows that a primitive 57^{th} root of unity is $\beta = \alpha^u$. where $u = (2^{28} - 1)/57 = 4,709$. The generator polynomial $g(x)$ is defined by,

$$g(x) = \prod_{i \in Q_{57}} (x - \beta^i)$$

$$= x^{28} + x^{26} + x^{24} + x^{23} + x^{22} + x^{21} + x^{19} + x^{15} + x^{14} + x^{13} + x^{12} + x^7 + x^6 + x^5 + x^3 + x^2 + x + 1$$

where the multiplicative order of the integer 2 modulo the code length $n = 57$ is represented by the degree of $g(x)$ which is 28. So, $2^{28} \equiv 1 (mod\, 57)$ and where $g(\beta) = 0$. An error pattern is considered correctable for the (57, 29, 17) QR Code if its weight is less than or equal to the error-correcting capacity $t = \frac{17-1}{2} = 8$. Let us now consider a noisy channel and the codeword

$$c(x) = c_0 + c_1x + c_2x^2 + \cdots + c_{56}x^{56}$$

$$e(x) = e_0 + e_1x + e_2x^2 + \cdots + e_{56}x^{56}$$

$$r(x) = r_0 + r_1x + r_2x^2 + \cdots + r_{56}x^{56}$$

respectively, correspond to the error pattern and the received vector. Next, the word that was received takes the form $r(x) = c(x) + e(x)$. Define $S_i = r(\beta^i) = e(\beta^i), i \in Q_{57}$ as the set of known syndromes that can be immediately computed by evaluating $r(x)$ at the roots of $g(x)$. These syndromes are referred to be unknown syndromes if i is absent from the set Q_{57}. It is said that the syndrome s_i is a known syndrome if $i \in Q_{57}$. If not, it's referred to as an unidentified syndrome. The unidentified syndromes are discovered in (2). There is a relationship between the syndromes and the QR code, $S_{2i} = S_i^2$, with indices modulo n. such as, $S_2 = S_1^2$, $S_4 = S_2^2 = S_1^4$, $S_8 = S_4^2 = S_1^8$, $S_{16} = S_8^2 = S_1^{16}$, $S_{64} = S_{32}^2 = S_1^{64}$, $S_{128} = S_{64}^2 = S_1^{128}$, $S_{256} = S_{128}^2 = S_1^{256}$. The error locator patterns is defined by,

$$L(z) = \prod_{i=1}^{v}(z - z_i) = z^v + \sum_{j=1}^{v} \sigma_j z^{v-j} \qquad (3)$$

$\sigma_1 = z_1 + z_2 + \cdots + z_v$
$\sigma_2 = z_1z_2 + z_1z_3 \ldots z_{v-1}z_v$
$\sigma_3 = z_2z_3 + z_2z_4 \ldots z_{2v}$
.
.
.
$\sigma_v = z_1z_2 \ldots z_v$

Thus, by using the Chien search algorithms to locate the error $z_1z_2 \ldots z_v$ as roots of polynomial $L(z)$ in (3), it is easy to find the elementary symmetric functions σ_i.The coefficients of $L(z)$ are found using the following Newton Identities:

$s_1 + \sigma_1 = 0$
$s_2 + \sigma_1 s_1 + 2\sigma_2 = 0$
$s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 = 0$
.
.
.
$s_v + \sigma_1 s_{v-1} + \ldots + \sigma_{v-1} s_1 + v\sigma_v = 0$

The decoding algorithm is used to decode the QR code up to 8 errors. The $S_1, S_2, \ldots, S_{16}$ syndromes are the first 16 in succession. However, only the syndromes S_1, S_4, S_6, S_7, S_9, S_{11}, S_{16} can be calculated directly from $r(x)$ and the others S_2, S_3, S_5, S_8, S_{10}, S_{12}, S_{13}, S_{14}, S_{15} are not determined directly from $r(x)$, which can be expressed in powers of S_2 and S_{15}.

4. Decoding algorithm for (57, 29, 17) QR code

One can apply the decoding algorithm to the receive data bits to recover the original error. A new decoding algorithm for the code is given below.

Step 1: The first 16 consecutive syndromes $S_1, S_2 \ldots \ldots, S_{16}$.
Step 2: Obtain the known syndromes $S_1, S_4, S_6, S_7, S_9, S_{11}, S_{16}$.
Step 3: If odd syndromes are zero, (i.e.) $S_1 = S_7 = S_9 = S_{11} = 0$, assume no errors occur and stop.
Step 4: Choose the unknown syndromes and set $v = 1$.
Step 5: Choose a subset $I = i_1, i_2, \ldots, i_{v+1} \subset Q$.
Step 6: Choose a subset J containing $v + 1$ elements from the difference set in Step 4. If all the possible sets J have been returning to Step 2.
Step 7: If the intersection of the multi-set $I \bigoplus J$ is empty, return to Step 4.
Step 8: Computing the consecutive unknown syndromes for possible pair S_2^v, S_{15}^v.
Step 9: If there exists one monomial of the unknown syndrome whose coefficient is 1 and whose power is different from that of other monomials, then stop; otherwise, return to Step 4.

4.1 Determination of Unknown syndromes

Assume that v errors occur in the received word. Let $I = i_1, i_2, \ldots i_{v+1}$ and $J = j_1, j_2, \ldots j_{v+1}$ denote two subsets of 0,1, 2...56, respectively. Next, consider the matrix (I, J) of size $(v + 1) \times (v + 1)$ given by,

$$S(I,J) = \begin{bmatrix} S_{i_1+j_1} & \cdots & S_{i_1+j_{v+1}} \\ \vdots & \ddots & \vdots \\ S_{i_{v+1}+j_1} & \cdots & S_{i_{v+1}+j_{v+1}} \end{bmatrix}$$

where the summation of the indices of the is modulo n and the rank of $S(I,J)$ is at most v, which in turn implies the following equation,

$$det\, S(I,J) = 0 \qquad (4)$$

Now, assuming the subsets I and J for the code,

$$I \bigoplus J = \{(i+j) \bmod 57 | i \in I, j \in J\}$$

Example: The sum of two subsets I and J are illustrated below.
If $v = 5, I = \{0,1,2,3,4\}$ and $J = \{1,2,3,4,5\}$, then

$$I \bigoplus J = \{0+1, 0+2, 0+3, 0+4, 0+5, 1+1, 1+2, 1+3, 1+4, 1+5, 2+1, 2+2, 2+3, 2+4, 2+5, 3+1, 3+2, 3+3, 3+4, 3+5, 4+1, 4+2, +4+3, 4+4, 4+5$$

Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 31 No. 2s (2024)

$I \oplus J = \{1,2,2,3,3,3,4,4,4,4,5,5,5,5,5,6,6,6,6,7,7,7,8,8,9\}$

It was proposed to find the corresponding subsets I and J. The following steps are involved in the determination of unknown syndromes,

Case 0: (zero error) No error in the received codeword if $S_1 = 0$; Otherwise goto case 1.

Case 1: (One error) $S_2 = S_1^2, S_{15} = S_1^{15}$

Case 2: (Two errors) Let $I_1 = \{0,4,1\}$, $J_1 = \{7,0,1\}$, $I_2 = \{0,4,7\}$, $J_2 = \{3,0,8\}$. The matrices are,

$$S(I_1,J_1) = \begin{pmatrix} S_7 & S_0 & S_1 \\ S_{11} & S_4 & \boldsymbol{S_5} \\ S_4 & S_1 & \boldsymbol{S_2} \end{pmatrix}$$

$$S(I_2,J_2) = \begin{pmatrix} S_3 & S_0 & S_8 \\ S_7 & S_4 & S_{12} \\ S_{10} & S_7 & \boldsymbol{S_{15}} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)(det\,(S(I_2,J_2)))\ is\ S_2^1, S_{15}^1$.

Case 3: (Three errors) Let $I_1 = \{7,0,1,2\}$, $J_1 = \{9,2,1,0\}$, $I_2 = \{11,7,8,10\}$, $J_2 = \{9,8,7,5\}$. The matrices are,

$$S(I_1,J_1) = \begin{pmatrix} S_{16} & S_9 & \boldsymbol{S_8} & S_7 \\ S_9 & \boldsymbol{S_2} & S_1 & S_0 \\ \boldsymbol{S_{10}} & \boldsymbol{S_3} & \boldsymbol{S_2} & S_1 \\ S_{11} & S_4 & \boldsymbol{S_3} & \boldsymbol{S_2} \end{pmatrix}$$

$$S(I_2,J_2) = \begin{pmatrix} \boldsymbol{S_{20}} & S_{19} & \boldsymbol{S_{18}} & S_{16} \\ S_{16} & \boldsymbol{S_{15}} & \boldsymbol{S_{14}} & \boldsymbol{S_{12}} \\ \boldsymbol{S_{17}} & S_{16} & \boldsymbol{S_{15}} & \boldsymbol{S_{13}} \\ S_{19} & \boldsymbol{S_{18}} & \boldsymbol{S_{17}} & \boldsymbol{S_{15}} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)(det\,(S(I_2,J_2)))\ is\ S_2^3, S_{15}^3$.

Case 4: (Four errors) Let $I_1 = \{0,2,1,4,3\}$, $J_1 = \{2,0,1,6,9\}$, $I_2 = \{0,9,1,15,4\}$, $J_2 = \{15,6,14,0,11\}$. The matrices are,

$$S(I_1,J_1) = \begin{pmatrix} \boldsymbol{S_2} & S_0 & S_1 & S_6 & S_9 \\ S_4 & \boldsymbol{S_2} & \boldsymbol{S_2} & \boldsymbol{S_8} & S_{11} \\ \boldsymbol{S_2} & S_1 & \boldsymbol{S_2} & S_7 & \boldsymbol{S_{10}} \\ S_6 & S_4 & \boldsymbol{S_5} & \boldsymbol{S_{10}} & \boldsymbol{S_{13}} \\ \boldsymbol{S_5} & \boldsymbol{S_3} & S_4 & S_9 & \boldsymbol{S_{12}} \end{pmatrix}$$

$$S(I_2,J_2)=\begin{pmatrix} \boldsymbol{S_{15}} & S_6 & \boldsymbol{S_{14}} & S_0 & S_{11} \\ S_{24} & \boldsymbol{S_{15}} & \boldsymbol{S_{23}} & S_9 & \boldsymbol{S_{20}} \\ S_{16} & S_7 & \boldsymbol{S_{15}} & S_1 & \boldsymbol{S_{12}} \\ S_{30} & S_{21} & \boldsymbol{S_{29}} & \boldsymbol{S_{15}} & \boldsymbol{S_{26}} \\ S_{19} & \boldsymbol{S_{10}} & S_{18} & S_4 & \boldsymbol{S_{15}} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)(det\ (S(I_2,J_2)))\ is\ S_2^5, S_{15}^5$.

Case 5: (Five errors) Let $I_1=\{1,0,12,2,20,40\}, J_1=\{1,2,13,0,5,3\}, I_2=\{15,6,2,45,32,1\},\ J_2=\{0,9,13,20,29,55\}$. The matrices are,

$$S(I_1,J_1)=\begin{pmatrix} \boldsymbol{S_2} & \boldsymbol{S_3} & \boldsymbol{S_{14}} & S_1 & S_6 & S_4 \\ S_1 & \boldsymbol{S_2} & \boldsymbol{S_{13}} & S_0 & \boldsymbol{S_5} & \boldsymbol{S_3} \\ \boldsymbol{S_{13}} & \boldsymbol{S_{14}} & S_{25} & \boldsymbol{S_{12}} & \boldsymbol{S_{17}} & \boldsymbol{S_{15}} \\ \boldsymbol{S_3} & S_4 & \boldsymbol{S_{15}} & \boldsymbol{S_2} & S_7 & \boldsymbol{S_{15}} \\ S_{21} & \boldsymbol{S_{22}} & \boldsymbol{S_{33}} & \boldsymbol{S_{20}} & S_{25} & \boldsymbol{S_{23}} \\ S_{41} & S_{42} & S_{53} & \boldsymbol{S_{40}} & S_{45} & S_{43} \end{pmatrix}$$

$$S(I_2,J_2)=\begin{pmatrix} \boldsymbol{S_{15}} & S_{24} & S_{28} & \boldsymbol{S_{35}} & \boldsymbol{S_{44}} & \boldsymbol{S_{13}} \\ S_6 & \boldsymbol{S_{15}} & S_{19} & \boldsymbol{S_{26}} & \boldsymbol{S_{35}} & \boldsymbol{S_4} \\ \boldsymbol{S_2} & S_{11} & \boldsymbol{S_{15}} & \boldsymbol{S_{22}} & S_{31} & S_{57} \\ S_{45} & S_{54} & S_1 & \boldsymbol{S_8} & \boldsymbol{S_{17}} & S_{43} \\ \boldsymbol{S_{32}} & S_{41} & S_{45} & \boldsymbol{S_{52}} & S_4 & S_{30} \\ S_1 & \boldsymbol{S_{10}} & \boldsymbol{S_{14}} & S_{21} & S_{30} & \boldsymbol{S_{56}} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)(det\ (S(I_2,J_2)))\ is\ S_2^4, S_{15}^3$.

Case 6: (Six errors) Let $I_1=\{2,0,1,50,47,21,12\}, J_1=\{0,2,1,19,16,4,50\}, I_2=\{13,1,0,11,39,51,4\},\ J_2=\{2,14,15,8,45,7,18\}$. The matrices are,

$$S(I_1,J_1)=\begin{pmatrix} \boldsymbol{S_2} & S_4 & S_3 & S_{21} & \boldsymbol{S_{18}} & S_6 & S_{52} \\ S_0 & \boldsymbol{S_2} & S_1 & S_{19} & S_{16} & S_4 & \boldsymbol{S_{50}} \\ S_1 & \boldsymbol{S_3} & \boldsymbol{S_2} & \boldsymbol{S_{20}} & S_{17} & \boldsymbol{S_5} & S_{51} \\ \boldsymbol{S_{50}} & \boldsymbol{S_{52}} & S_{51} & \boldsymbol{S_{12}} & S_9 & S_{54} & S_{43} \\ \boldsymbol{S_{47}} & S_{49} & \boldsymbol{S_{48}} & S_9 & S_6 & S_{51} & \boldsymbol{S_{40}} \\ S_{21} & \boldsymbol{S_{23}} & \boldsymbol{S_{22}} & \boldsymbol{S_{40}} & \boldsymbol{S_{37}} & S_{25} & \boldsymbol{S_{14}} \\ \boldsymbol{S_{12}} & \boldsymbol{S_{14}} & \boldsymbol{S_{13}} & S_{31} & S_{28} & S_{16} & \boldsymbol{S_5} \end{pmatrix}$$

$$S(I_2,J_2)=\begin{pmatrix} \boldsymbol{S_{15}} & \boldsymbol{S_{27}} & S_{28} & S_{21} & S_1 & \boldsymbol{S_{20}} & S_{31} \\ \boldsymbol{S_3} & \boldsymbol{S_{15}} & S_{16} & S_9 & \boldsymbol{S_{46}} & \boldsymbol{S_8} & S_{19} \\ \boldsymbol{S_2} & S_4 & \boldsymbol{S_{15}} & \boldsymbol{S_8} & S_{45} & S_7 & \boldsymbol{S_{18}} \\ \boldsymbol{S_{13}} & S_{25} & \boldsymbol{S_{26}} & S_{19} & \boldsymbol{S_{56}} & \boldsymbol{S_{18}} & S_{29} \\ S_{41} & \boldsymbol{S_{53}} & S_{54} & \boldsymbol{S_{47}} & \boldsymbol{S_{27}} & \boldsymbol{S_{46}} & S_{57} \\ \boldsymbol{S_{53}} & \boldsymbol{S_8} & S_9 & \boldsymbol{S_2} & S_{39} & \boldsymbol{S_1} & \boldsymbol{S_{12}} \\ S_6 & \boldsymbol{S_{18}} & S_{19} & \boldsymbol{S_{12}} & S_{49} & S_{11} & \boldsymbol{S_{22}} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)(det\ (S(I_2,J_2)))\ is\ S_2^3,S_{15}^3$.

Case 7: (Seven errors) Let $I_1=\{21,41,2,5,0,1,30,7\}$, $J_1=\{4,6,0,30,2,1,11,21\}$, $I_2=\{1,0,13,11,28,39,55,16\}$, $J_2=\{14,15,2,4,24,45,39,0\}$. The matrices are,

$$S(I_1,J_1)=\begin{pmatrix} S_{25} & \boldsymbol{S_{27}} & S_{21} & S_{51} & S_{23} & \boldsymbol{S_{22}} & \boldsymbol{S_{32}} & S_{42} \\ S_{45} & \boldsymbol{S_{47}} & S_{41} & \boldsymbol{S_{14}} & S_{43} & S_{42} & \boldsymbol{S_{52}} & \boldsymbol{S_{5}} \\ S_{6} & \boldsymbol{S_{8}} & \boldsymbol{S_{2}} & \boldsymbol{S_{32}} & S_{4} & \boldsymbol{S_{3}} & \boldsymbol{S_{13}} & \boldsymbol{S_{23}} \\ S_{9} & S_{11} & \boldsymbol{S_{5}} & \boldsymbol{S_{35}} & S_{7} & S_{6} & S_{16} & \boldsymbol{S_{26}} \\ S_{4} & S_{6} & S_{0} & S_{30} & \boldsymbol{S_{2}} & S_{1} & S_{11} & S_{21} \\ \boldsymbol{S_{5}} & S_{7} & S_{1} & S_{31} & \boldsymbol{S_{3}} & \boldsymbol{S_{2}} & \boldsymbol{S_{12}} & \boldsymbol{S_{22}} \\ \boldsymbol{S_{34}} & S_{36} & S_{30} & \boldsymbol{S_{3}} & \boldsymbol{S_{32}} & S_{31} & S_{41} & S_{51} \\ S_{11} & \boldsymbol{S_{13}} & S_{7} & \boldsymbol{S_{37}} & S_{9} & \boldsymbol{S_{8}} & \boldsymbol{S_{18}} & S_{28} \end{pmatrix}$$

$$S(I_2,J_2)=\begin{pmatrix} \boldsymbol{S_{15}} & S_{16} & \boldsymbol{S_{3}} & \boldsymbol{S_{5}} & S_{25} & \boldsymbol{S_{46}} & \boldsymbol{S_{40}} & S_{1} \\ \boldsymbol{S_{14}} & \boldsymbol{S_{15}} & \boldsymbol{S_{2}} & S_{4} & S_{24} & S_{45} & S_{39} & S_{0} \\ \boldsymbol{S_{27}} & S_{28} & \boldsymbol{S_{15}} & \boldsymbol{S_{17}} & \boldsymbol{S_{37}} & S_{1} & \boldsymbol{S_{52}} & \boldsymbol{S_{13}} \\ S_{25} & \boldsymbol{S_{26}} & \boldsymbol{S_{13}} & \boldsymbol{S_{15}} & \boldsymbol{S_{35}} & \boldsymbol{S_{56}} & \boldsymbol{S_{50}} & S_{11} \\ S_{42} & S_{43} & S_{30} & \boldsymbol{S_{32}} & \boldsymbol{S_{52}} & S_{16} & \boldsymbol{S_{10}} & S_{28} \\ \boldsymbol{S_{53}} & S_{54} & \boldsymbol{S_{41}} & S_{43} & S_{6} & S_{28} & S_{21} & S_{39} \\ \boldsymbol{S_{12}} & \boldsymbol{S_{13}} & \boldsymbol{S_{57}} & \boldsymbol{S_{2}} & \boldsymbol{S_{22}} & S_{43} & \boldsymbol{S_{37}} & S_{55} \\ S_{30} & S_{31} & \boldsymbol{S_{18}} & S_{20} & \boldsymbol{S_{40}} & S_{4} & S_{55} & S_{16} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)(det\ (S(I_2,J_2)))\ is\ S_2^3,S_{15}^4$.

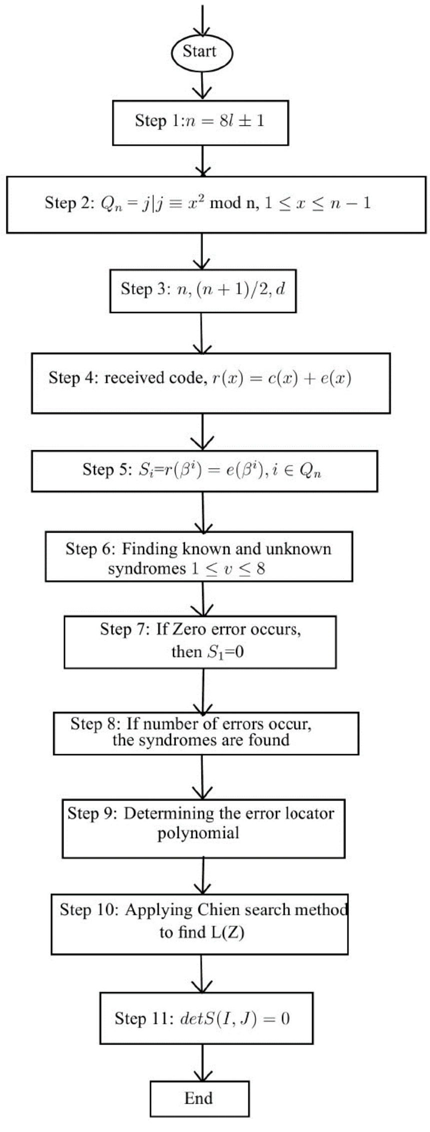
Case 8: (Eight errors) Let $I_1=\{51,0,2,1,8,49,11,21,3\}$, $J_1=\{8,2,0,1,51,4,55,5,3\}$, $I_2=\{0,1,13,51,28,4,16,9,31\}$, $J_2=\{15,14,2,21,11,13,6,1,3\}$. The matrices are,

$$S(I_1,J_1)=\begin{pmatrix} \boldsymbol{S_{2}} & \boldsymbol{S_{53}} & S_{51} & \boldsymbol{S_{52}} & S_{45} & S_{55} & S_{49} & \boldsymbol{S_{56}} & S_{54} \\ \boldsymbol{S_{8}} & \boldsymbol{S_{2}} & S_{0} & S_{1} & S_{51} & S_{4} & S_{55} & \boldsymbol{S_{5}} & \boldsymbol{S_{3}} \\ \boldsymbol{S_{10}} & S_{4} & \boldsymbol{S_{2}} & \boldsymbol{S_{3}} & \boldsymbol{S_{53}} & S_{6} & S_{57} & S_{7} & \boldsymbol{S_{5}} \\ S_{9} & \boldsymbol{S_{3}} & S_{1} & \boldsymbol{S_{2}} & \boldsymbol{S_{52}} & \boldsymbol{S_{5}} & \boldsymbol{S_{56}} & S_{6} & S_{4} \\ S_{9} & \boldsymbol{S_{10}} & \boldsymbol{S_{8}} & S_{9} & \boldsymbol{S_{2}} & S_{12} & S_{6} & \boldsymbol{S_{13}} & S_{11} \\ S_{16} & S_{51} & S_{49} & \boldsymbol{S_{50}} & S_{43} & \boldsymbol{S_{53}} & \boldsymbol{S_{47}} & S_{54} & \boldsymbol{S_{52}} \\ S_{57} & \boldsymbol{S_{13}} & S_{11} & S_{12} & S_{5} & S_{15} & S_{9} & S_{16} & S_{14} \\ \boldsymbol{S_{29}} & \boldsymbol{S_{23}} & S_{21} & \boldsymbol{S_{22}} & \boldsymbol{S_{15}} & S_{25} & S_{19} & \boldsymbol{S_{26}} & S_{24} \\ S_{11} & \boldsymbol{S_{5}} & \boldsymbol{S_{3}} & \boldsymbol{S_{34}} & S_{54} & S_{7} & S_{1} & \boldsymbol{S_{8}} & S_{6} \end{pmatrix}$$

$$S(I_2,J_2)=\begin{pmatrix} \boldsymbol{S_{15}} & \boldsymbol{S_{14}} & \boldsymbol{S_{2}} & S_{21} & S_{11} & \boldsymbol{S_{13}} & S_{6} & S_{1} & \boldsymbol{S_{3}} \\ S_{16} & \boldsymbol{S_{15}} & \boldsymbol{S_{3}} & \boldsymbol{S_{22}} & \boldsymbol{S_{12}} & \boldsymbol{S_{14}} & S_{7} & \boldsymbol{S_{2}} & S_{4} \\ S_{28} & \boldsymbol{S_{27}} & \boldsymbol{S_{15}} & \boldsymbol{S_{34}} & S_{24} & \boldsymbol{S_{26}} & S_{19} & \boldsymbol{S_{14}} & S_{16} \\ S_{9} & \boldsymbol{S_{8}} & \boldsymbol{S_{53}} & \boldsymbol{S_{15}} & \boldsymbol{S_{5}} & S_{7} & S_{57} & \boldsymbol{S_{52}} & S_{54} \\ S_{43} & S_{42} & S_{30} & S_{49} & S_{39} & S_{41} & \boldsymbol{S_{34}} & \boldsymbol{S_{29}} & S_{31} \\ S_{19} & \boldsymbol{S_{18}} & S_{6} & S_{25} & \boldsymbol{S_{15}} & \boldsymbol{S_{17}} & \boldsymbol{S_{10}} & \boldsymbol{S_{5}} & S_{7} \\ S_{31} & S_{30} & \boldsymbol{S_{18}} & \boldsymbol{S_{37}} & \boldsymbol{S_{27}} & \boldsymbol{S_{29}} & \boldsymbol{S_{22}} & \boldsymbol{S_{17}} & S_{19} \\ S_{24} & \boldsymbol{S_{23}} & S_{11} & S_{30} & \boldsymbol{S_{20}} & \boldsymbol{S_{22}} & \boldsymbol{S_{15}} & \boldsymbol{S_{10}} & \boldsymbol{S_{12}} \\ S_{46} & S_{45} & \boldsymbol{S_{33}} & \boldsymbol{S_{52}} & S_{42} & \boldsymbol{S_{44}} & S_{37} & \boldsymbol{S_{32}} & \boldsymbol{S_{34}} \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)\left(det\left(S(I_2,J_2)\right)\right)\ is\ S_2^5,S_{15}^4$.

The above conviction is described in the following flowchart:



5. Application for the algorithm

The algorithm has been successfully implemented to the provided example, resulting in enhanced performance and efficiency. Let $(17,9,5)$ QR code over $GF(2^8)$ generated by the primitive polynomial $x^8 + x^6 + x^5 + x + 1$. The set $Q_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$. Therefore $\beta = \alpha^u$ is a primitive 17^{th} root of unity and $u = (2^8 - 1)/17 = 15$. This code can correct upto two errors.

For two error cases, $0 \leq v \leq 2$.

For $v = 1$, $I_1 = \{1,4\}, J_1 = \{2,1\}$. The matrices are,

$$S(I_1,J_1) = \begin{pmatrix} \boldsymbol{S_3} & S_2 \\ S_6 & S_5 \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)$ is S_3^1.

For $v = 2$, $I_1 = \{2,1,8\}, J_1 = \{4,2,1\}$. The matrices are,

$$S(I_1,J_1) = \begin{pmatrix} S_6 & S_4 & \boldsymbol{S_3} \\ S_5 & \boldsymbol{S_3} & S_2 \\ S_{12} & S_{10} & S_9 \end{pmatrix}$$

The corresponding monomial in $det\left(S(I_1,J_1)\right)$ is S_3^2.

Assume the message polynomial $I(x) = x^5 + x + 1$ and the code polynomial $c(x) = x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^4 + x^2 + x^1 + x + 1$. Two error cases are given below.

Case 1: For one error, assume the error polynomial $e(x) = x^3$ and the received polynomial is, $r(x) = x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^5 + x^3 + x + 1$. Unknown syndrome for one error $S_3^1 = \alpha^{14}$. The error locator polynomial $L(z) = 1 + \alpha^{18}x$. The root of the $\sigma(x)$ is $x_1 = \alpha^7$ and the error polynomial $e(x) = x^3$.

Case 2: For two error, assume the error polynomial $e(x) = x^3 + x^2$ and the received polynomial is, $r(x) = x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^5 + x^3 + x + 1$. Unknown syndrome for two error $S_3^2 = \alpha^{16}$. The error locator polynomial $L(z) = 1 + \alpha^{12}x$. The root of the $\sigma(x)$ is $x_1 = \alpha^8$ and the error polynomial $e(x) = x^3 + x^2$.

6. Conclusion

In this manuscript, we present an original non-binary quadratic residue code characterized by parameters (57, 29, 17), operating within a binary field. Our approach involves the adaptation of methods analogous to those employed in discerning unknown syndromes within binary quadratic residue codes, tailored for this non-binary code of length 57. By meticulously selecting suitable subsets and index sets, we effectively tackle eight instances of errors, subsequently resolving them with the aid of a pioneering decoding algorithm. Furthermore, we develop into the practical application of this algorithm within our study.

References:

[1] Chen X, I S Reed, T K Truong, Decoding the (73, 37, 13) quadratic residue code, IEEE Proceedings - Computers and Digital Techniques, 141(5), September 1994.
[2] Elia M, Algebraic decoding of the (23,12,7) Golay codes, IEEE Trans.Inf.Theory, 33(1), Jan 1987.
[3] Hung Peng Lee, Hsin Chiu Chang, Modified algebraic decoding of the binary (47, 24, 11) quadratic residue code, 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), 16 May 2011.
[4] Li Y, H Liu, Q Chen and T K Truong, Algebraic and linear programming decoding of the (73, 37, 13) quadratic residue code, IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 2014.
[5] Lin T C, 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, 2010.
[6] Lin Wang, Young Li, Trieu Kien, Tsung Ching, On Decoding of the (89,45,17) Quadratic Residue Code, IEEE Transactions on Communication, 61(3), March 2013.
[7] Macwiilliams F J and N J A Sloane, The Theory of Error-Correcting Codes (First edition), Bell Laboratories, Murray Hill, U.S.A, 1977.
[8] Mita A, On the Construction of m-Sequences via Primitive Polynomials with a Fast Identification Method, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering, 25 September 2008.
[9] Pengwei Zhang, Yong Li, Hsin Chiu Chang, Hongqing Liu, Trieu-Kien Truong, Fast Decoding of the (47, 24, 11) Quadratic Residue Code Without Determining the Unknown Syndromes, IEEE Communications Letters, 19(8), August 2015.
[10] Pless V S, Zhongqiang Qian, Cyclic codes and quadratic residue codes over Z4, IEEE Transactions on Information Theory, 42(5), September 1996.
[11] Prange, Some cyclic error-correcting codes with simple decoding algorithms, Air Force Cambridge Research Center TN, 1958.
[12] Ruhua He, Irving S. Reed, Trieu-Kien Truong, Xuemin Chen, Decoding the (47,24,11) Quadratic Residue Code, IEEE Transactions on Communications, 47(3), March 2001.
[13] Shapiro H.S, D.L.Slotnick, On the Mathematical Theory of Error-Correcting Codes, IBM Journal of Research and Development, 3(1), January 1959.
[14] Todd K.Moon, Error Correction Coding: Mathematical Methods and Algorithms, John Wiley and Sons Inc, USA, 2014.
[15] Tsung-Ching Lin, Trieu-Kien Truong, Hung-Peng Lee , Hsin-Chiu Chang, Algebraic decoding of the (41, 21, 9) Quadratic Residue codes, Information Sciences, 179(19), 9 September 2009.
[16] Wen-Ku Su, Pei-Yu Shih, Tsung-Ching Lin, and Trieu-Kien Truong, Decoding of the (48,24, 12) Extended Quadratic Residue Code up to Six Errors, International Conference on Communications, Circuits and Systems, 2008.
[17] Xuemin Chen, I.S. Reed, T.K. Truong, A performance comparison of the binary quadratic residue codes with the 1/2-rate convolutional codes, IEEE Transactions on Information Theory, 40(1), January 1994.
[18] Yaotsu Chang, Trieu-Kien Truong, Algebraic Decoding of (71, 36, 11), (79,40, 15), and (97, 49, 15) Quadratic Residue Codes, IEEE Transaction on Communication, 51(9), September 2003.
[19] Zhang.P, Y. Li, H.C. Chang, H. Liu and T.K. Truong, Fast Decoding of the (47, 24, 11) Quadratic Residue Code Without Determining the Unknown Syndromes, IEEE Communications Letters, 19(8), August 2015.