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

P. Shakila Banu, R. Shobana

aAssistant Professor, Department of Mathematics, Vellalar College for Women, Erode-638012, Tamilnadu, India
bResearch 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 methodology 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 decoding algorithm.

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


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].

A.H.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 \( v \geq 6 \) 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 \( c = (c_0,c_1,\ldots,c_{n-1}) \) in \( C \), its right cyclic shift \( c = (c_{n-1},c_0,\ldots,c_{n-2}) \) 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 \( N_p, Q, N \) 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 \( GF(l) \), \( \alpha \) 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 \( n - k \), \( g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k} \).
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 \( (n, \frac{n+1}{2}, d) \) 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,
\[
Q_n = \{ j | j \equiv x^2 \mod n, \ 1 \leq x \leq n-1 \} \quad (1)
\]
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
\[
Q_{57} = \{1,4,6,7,9,11,16,19,21,24,25,28,30,31,36,39,41,42,43,45,49,51,54,55\} \quad (2)
\]
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 \( \alpha \). It follows that a primitive 57\textsuperscript{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 \( t = \frac{\frac{17-1}{2}}{2} = 8 \). Let us now consider a noisy channel and the codeword.
The syndromes are referred to as an unidentified syndrome if \( i \in Q_{57} \) 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 \( i \in Q_{57} \). 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, \( S_2 = S_1^2 \), \( S_4 = S_2^2 = S_4^4 \), \( S_8 = S_4^2 = S_8^4 \), \( S_{16} = S_8^2 = S_1^{16} \), \( S_{64} = S_{32}^2 = S_1^{64} \), \( S_{128} = S_{64}^2 = S_{128}^{28} \), \( S_{256} = S_{128}^2 = S_1^{256} \). The error locator patterns is defined by,

\[
L(z) = \prod_{i=1}^{\nu}(z - z_i) = z^\nu + \sum_{j=1}^{\nu} \sigma_j z^{\nu-j} \tag{3}
\]

\[
\begin{align*}
\sigma_1 &= z_1 + z_2 + \cdots + z_\nu \\
\sigma_2 &= z_1 z_2 + z_1 z_3 \cdots z_{\nu-1} z_\nu \\
\sigma_3 &= z_1 z_2 z_3 \cdots z_\nu \\
&\vdots \\
\sigma_\nu &= z_1 z_2 \cdots z_\nu 
\end{align*}
\]

Thus, by using the Chien search algorithms to locate the error \( z_1 z_2 \cdots z_\nu \) as roots of polynomial \( L(z) \) in (3), it is easy to find the elementary symmetric functions \( \sigma_i \).The coefficients of \( L(z) \) are found using the following Newton Identities:

\[
\begin{align*}
s_1 + \sigma_1 &= 0 \\
s_2 + \sigma_1 s_1 + 2\sigma_2 &= 0 \\
s_3 + \sigma_1 s_2 + \sigma_2 s_1 + 3\sigma_3 &= 0 \\
&\vdots \\
s_\nu + \sigma_1 s_{\nu-1} + \cdots + \sigma_{\nu-1} s_1 + \nu\sigma_\nu &= 0 
\end{align*}
\]

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 \( S_1, S_4, S_5, S_7, S_9, S_{11}, S_{16} \) 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 \( S_1, S_2, \ldots, S_{16} \).

**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 \( I \oplus J \) is empty, return to Step 4.

**Step 8:** Computing the consecutive unknown syndromes for possible pair \( S_{15}^I, S_{15}^J \).

**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,

\[
det S(I, J) = 0 \quad (4)
\]

Now, assuming the subsets \( I \) and \( J \) for the code,

\[
I \oplus J = \{(i + j) \mod 57 | i \in I, j \in J\}
\]

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

\[
I \oplus J = \{0 + 1, 0 + 2, 0 + 3, 0 + 4, 0 + 5, 1 + 1, 1 + 2, 1 + 3, 1 + 4, 1 + 5, 2 + 1, 2 + 2, 2 + 3, 2 + 4, 2 + 5, 3 + 1, 3 + 2, 3 + 3, 3 + 4, 3 + 5, 4 + 1, 4 + 2, 4 + 3, 4 + 4, 4 + 5\}
\]
\( I \oplus J = \{1, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 5, 6, 6, 6, 6, 7, 7, 7, 8, 8, 9\} \)

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,

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

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

The corresponding monomial in \( \text{det} \ (S(I_1, J_1)) \) (det (\( S(I_2, J_2) \))) is \( S_1^1, S_1^{15} \).

**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,

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

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

The corresponding monomial in \( \text{det} \ (S(I_1, J_1)) \) (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,

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

https://internationalpubls.com
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,

$$S(I_1, J_1) = \begin{pmatrix}
S_{15} & S_6 & S_{14} & S_0 & S_{11} \\
S_{24} & S_{15} & S_{23} & S_0 & S_{20} \\
S_{16} & S_7 & S_{15} & S_1 & S_{12} \\
S_{30} & S_{21} & S_{29} & S_{15} & S_{26} \\
S_{19} & S_{10} & S_{18} & S_4 & S_{15}
\end{pmatrix}$$

The corresponding monomial in $det \left(S(I_1, J_1)\right) \left(det \left(S(I_2, J_2)\right)\right)$ is $S^5_{12}, S^5_{15}$.

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

$$S(I_1, J_1) = \begin{pmatrix}
S_{15} & S_{24} & S_{28} & S_{35} & S_{44} & S_{13} \\
S_{6} & S_{15} & S_{19} & S_{26} & S_{35} & S_{4} \\
S_{2} & S_{11} & S_{15} & S_{22} & S_{31} & S_{57} \\
S_{45} & S_{54} & S_{1} & S_{8} & S_{17} & S_{43} \\
S_{32} & S_{41} & S_{45} & S_{52} & S_{4} & S_{30} \\
S_{1} & S_{10} & S_{14} & S_{21} & S_{30} & S_{56}
\end{pmatrix}$$

The corresponding monomial in $det \left(S(I_1, J_1)\right) \left(det \left(S(I_2, J_2)\right)\right)$ is $S^4_{2}, S^3_{15}$.
The corresponding monomial in $\det (S(I_1,J_1)) (\det (S(I_2,J_2)))$ is $S_2^3 S_{15}^3$.

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

$$
S(I_1,J_1) = \begin{pmatrix}
S_{25} & S_{27} & S_{21} & S_{51} & S_{23} & S_{22} & S_{32} & S_{42} \\
S_{45} & S_{47} & S_{41} & S_{14} & S_{43} & S_{42} & S_{52} & S_5 \\
S_6 & S_8 & S_2 & S_{32} & S_4 & S_3 & S_{13} & S_{23} \\
S_9 & S_{11} & S_5 & S_{35} & S_7 & S_6 & S_{16} & S_{26} \\
S_4 & S_6 & S_0 & S_{30} & S_2 & S_1 & S_{11} & S_{21} \\
S_5 & S_7 & S_1 & S_{31} & S_3 & S_2 & S_{12} & S_{22} \\
S_{34} & S_{36} & S_{30} & S_3 & S_{32} & S_{31} & S_{41} & S_{51} \\
S_{11} & S_{13} & S_7 & S_{37} & S_9 & S_8 & S_{18} & S_{28}
\end{pmatrix}
$$

$$
S(I_2,J_2) = \begin{pmatrix}
S_{15} & S_{16} & S_3 & S_5 & S_{25} & S_{46} & S_{40} & S_1 \\
S_{14} & S_{15} & S_2 & S_4 & S_{24} & S_{45} & S_{39} & S_0 \\
S_{27} & S_{28} & S_{15} & S_{17} & S_{37} & S_1 & S_{52} & S_{13} \\
S_{25} & S_{26} & S_{13} & S_{15} & S_{35} & S_{56} & S_{50} & S_{11} \\
S_{42} & S_{43} & S_{30} & S_{32} & S_{52} & S_{16} & S_{10} & S_{28} \\
S_{53} & S_{54} & S_{41} & S_{43} & S_6 & S_{28} & S_{21} & S_{29} \\
S_{12} & S_{13} & S_{57} & S_2 & S_{22} & S_{43} & S_{37} & S_{55} \\
S_{30} & S_{31} & S_{18} & S_{20} & S_{40} & S_4 & S_{55} & S_{16}
\end{pmatrix}
$$

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

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

$$
S(I_1,J_1) = \begin{pmatrix}
S_2 & S_{53} & S_{51} & S_{52} & S_{45} & S_{55} & S_{49} & S_{56} & S_{54} \\
S_8 & S_2 & S_0 & S_1 & S_{51} & S_4 & S_{55} & S_5 & S_3 \\
S_{10} & S_4 & S_2 & S_3 & S_{53} & S_6 & S_{57} & S_7 & S_5 \\
S_9 & S_3 & S_1 & S_2 & S_{52} & S_5 & S_{56} & S_6 & S_4 \\
S_9 & S_{10} & S_8 & S_9 & S_2 & S_{12} & S_6 & S_{13} & S_{11} \\
S_{16} & S_{51} & S_{49} & S_{50} & S_{43} & S_{53} & S_{47} & S_{54} & S_{52} \\
S_{57} & S_{13} & S_{11} & S_{12} & S_5 & S_{15} & S_9 & S_{16} & S_{14} \\
S_{29} & S_{23} & S_{21} & S_{22} & S_{15} & S_{25} & S_{19} & S_{26} & S_{24} \\
S_{11} & S_5 & S_3 & S_{34} & S_{54} & S_7 & S_1 & S_8 & S_6
\end{pmatrix}
$$

https://internationalpubls.com
The corresponding monomial in $\det (S(I_1, J_1)) \det (S(I_2, J_2))$ 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 up to 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,

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

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

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

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

The corresponding monomial in $\det(S(I_1,J_1))$ 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, $r(x) = x^{16} + x^{15} + x^{13} + x^9 + x^8 + x^4 + x^2 + x^1 + x + 1$. 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:


[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.


