International Journal of Computational Intelligence Research (IJCIR).
ISSN: 0973-1873 Volume 13, Number 8 (2017), pp. 2015–2027
© Research India Publications
http://www.ripublication.com/ijcir.htm

New Algebraic Decoding of (17,9,5) Quadratic Residue Code by using Inverse Free Berlekamp-Massey Algorithm (IFBM)

Renuka Sahu, B.P. Tripathi and S.K. Bhatt

Department of Mathematics,
Govt. N.P.G.College of Science,
Raipur (C.G.), India.

Abstract

In this paper a new algebraic decoding approach for (17,9,5) Quadratic Residue Code is proposed by using the Inverse Free Berlekamp-Massey Algorithm i.e. IFBM algorithm. By using an efficient algorithm an unknown syndrome are also developed in this paper. With the help of unknown syndromes, we achieve the alternative consecutive syndromes which are needed for the application of the Berlekamp-Massey algorithm. The decoding scheme developed here, is simpler to put into effect than the previous decoding algorithm developed for (17,9,5) QR code.

AMS subject classification: 94A60.
Keywords: Quadratic Residue Codes, Inverse free Berlekamp-Massey Algorithm, Unknown Syndromes, Known Syndromes.

1. Introduction

The well-known QR codes, introduced by way of Prange [1] in 1957, are cyclic BCH codes with code rates greater than or same to at least one-half. Similarly, the codes typically have large minimum distances in order that maximum of recognised QR codes are the exceptional-known codes. The code augmented by using a parity bit, as an instance, the (24, 12, 8) QR code became utilized to provide error control on the Voyager deep-space challange [2]. In the past decades, several decoding strategies were advanced to decode the binary QR codes. The Algebraic Decoding Algorithm's most used to decode the QR codes are the Newton's identities with either Sylvester resultants [3]-[10] or Gröbner bases [11], or inverse-free Berlekamp-Massey (IFBM) algorithm [12]-[16] to determine the error-locator polynomial. Amongst them, the ADA of the (17, 9, 5) QR code [16] can correct up to two errors within the finite field GF(2^8), due to tyhe fact the error-correcting capability of the code is $t = \lfloor (d-1)/2 \rfloor = \lfloor (5-1)/2 \rfloor = 2$ errors, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x, and $d = 5$ is the minimum Hamming distance of the code. In [16], the authors use the known syndrome S_1 to replace unknown syndromes. Furthermore, the coefficients of the error-locator polynomial are also replaced by S_1. Eventually, the Chien search algorithm [18] is implemented to find the roots of the error-locator polynomial.

Moreover, with a purpose to decrease the computational complexity in the power of syndrome, a fast multiplier algorithm given in [19] is utilized in C++ program. This technique can speed up the decoding procedure and make this proposed decoding algorithm easy to implement in software and hardware.

The rest parts of this paper are organized as follows: Section 2 gives the basic terminology of the QR codes and defines the unknown syndromes. Additionally, an efficient algorithm for calculating unknown syndromes is delivered in this section. Section 3 is the main body of this paper; it demonstrate the unknown syndrome technique, developed in section 2 as well as the inverse-free BM algorithm [12] to decode the (17,9,5) QR code. Ultimately, a completely work-outed example, using the (17,9,5) QR code is demonstrated in detail. The final section gives some concluding remarks about the decoding scheme developed in this paper.

2. Preliminary

2.1. Binary QR code [19]

A binary 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 $g(x)$ over $GF(2)$, where $k = (n+1)/2$ is the message length and n is the code length. Let n be a prime number of the form $n = 8m \pm 1$, where m is a positive integer and m be the smallest positive integer such that $2^m \equiv 1(\text{ mod n})$. The set Q_n of quadratic residues modulo n is the set of nonzero squares modulo n; that is, $Q_n = \{j \mid j \equiv x^2 \ mod \ n, 1 \leq x \leq (n-1)/2\}$. For the binary (17, 9, 5) QR code over $GF(2^8)$, the quadratic residue set Q_{17} is

$$Q_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\} \tag{1}$$

Let an element $\alpha \in GF(2^8)$ be a root of primitive polynomial $p(x) = x^8 + x^4 + x^3 + x^2 + 1$; that is, p($\alpha$) = 0. Obviously, the element $\beta = \alpha^u$, where $u = (2^m - 1)/n = (2^8 - 1)/17 = 15$, is a primitive 15-th root of unity in $GF(2^8)$. The generator polynomial g(x) is defined by

$$g(x) = \prod_{i \in Q_{17}} (x - \beta_i) = x^8 + x^5 + x^4 + x^3 + 1 \tag{2}$$

where the degree of g(x) is 8, which is the multiplicative order of the integer 2 modulo the code length 17; that is, $2^8 \equiv 1 \ mod \ 17$. If $\alpha = 2$, then $\beta = \alpha^{15} = 38$ and $g(\beta) = 0$. By cyclically shifting β once to the left and mod g(x), then one obtains the 17 roots of $x^{17} - 1$.

Since the codewords are a multiple of the g(x), the codeword polynomial of the (17, 9, 5) QR code can be represented by

$$c(x) = \sum_{i=0}^{16} = m(x)g(x),$$

where $c_i \in GF(2)$ for $0 \leq i \leq 16$, and

$$m(x) = m_8x^8 + \cdots + m_1x + m_0$$

denotes information polynomial, where $m_i \in GF(2)$ for $0 \leq i \leq 8$. In such a representation, this type of codeword is called the nonsystematic encoding. In practice, the encoding procedure is often implemented by the use of systematic encoding.

Let $p(x) = p_7x^7 + \cdots + p_1x + p_0$ be the parity-check polynomial, where $p_i \in GF(2)$ for $0 \leq i \leq 7$. Also, let $m(x)x^{n-k}$ divide by g(x), then we get the following identity:

$$m(x)x^{n-k} = q(x)g(x) + d(x). \tag{3}$$

Multiplying both sides of (3) by x^k and using $x^n = 1$, Then, it yields $d(x)x^k + m(x) = (q(x)x^k)g(x)$. The term $d(x)x^k + m(x)$, which is a multiple of g(x), has m(x) in its lower k bits and $p(x) = d(x)x^k$ in its higher $n - k$ bits. Thus, the codeword can be represented by the equation below.

$$c(x) = d(x)x^k + m(x) = p(x) + m(x). \tag{4}$$

As shown in (4), this form of the codeword is called systematic encoding. Now, let a codeword be transmitted through a noisy channel to obtain a received word of the form

$$r(x) = c(x) + e(x),$$

where $e(x) = e_{16}x^{16} + \cdots + e_1x + e_0$ is the occurred error polynomial and $e_i \in GF(2)$. For simplification, the polynomial form can be expressed as the vector form. For example, $c(x)$ can be expressed as $c = (c_{16}, \cdots, c_1, c_0)$. The syndromes or known syndromes of the code are defined by

$$S_i = r(\beta^i) = c(\beta^i) + e(\beta^i) = e(\beta^i) = \sum_{j=0}^{16} e_j(\beta^i)^j, \tag{5}$$

where $i(mod 17) \in Q_{17}$. If i not belongs to Q_{17}, the syndromes are called unknown syndromes. All known syndromes can be expressed as the power of S_1, such as, $S_2 = S_1^2$, $S_4 = S_1^4$, etc; thus, S_1 is called the primary unknown syndrome. Similarly, S_3 is called the primary unknown syndrome, such as, $S_6 = S_3^2, S_{12} = S_3^4$, etc. Note that $S_0 = 0 \; or \; 1$ depends on the fact that v is even or odd, where v is the actual number of errors to be corrected and $1 \leq v \leq 2$. If there are $v \leq t$ errors in $r(x)$, then $e(x)$ has v nonzero terms over $GF(2)$; that is,

$$e_{(x)} = x^{r1} + x^{r2} + \cdots + x^{r_v},$$

where $0 \leq r_1 < r_2 < \cdots < r_v \leq n-1$. For $i \in Q_n$, the syndrome can be written as

$$S_i = Z_1^i + Z_2^i + \cdots + Z_v^i, \tag{6}$$

where $Z_j = \beta^{r_j}$ for $1 \leq j \leq v$ are called the error locators. For the $(17, 9, 5)$ QR code, one has the following equalities among the known syndromes as:

$$S_2 = S_1^2, S_4 = S_1^{2^2}, S_8 = S_1^{2^3}, S_{16} = S_1^{2^4}, S_5 = S_1^{2^5}, S_{13} = S_1^{2^6}, S_9 = S_1^{2^7}$$

Assuming that v errors occur, the error-locator polynomial $L_v(x)$ is defined by

$$\sigma(z) = \prod_{j=1}^{v}(1 + Z_j z) = 1 + \sum_{j=1}^{v} \sigma_j z^j \tag{7}$$

where

$$\sigma_1 = Z_1 + Z_2 + \cdots + Z_v, \sigma_2 = Z_1 Z_2 + Z_1 Z_3 + \cdots + Z_{v-1} Z_v$$

$$= \sum_{1 \leq i < j \leq v} Z_i Z_j, \ldots,$$

and

$$\sigma_v = Z_1 Z_2 \cdots Z_v.$$

By applying the BM algorithm the error-locator polynomial can be obtained. It is well known that the BM algorithm is an efficient method for determining the error-locator polynomial which used to decode both the RS codes and BCH codes. In this paper, we uses it to decode both the $(17, 9, 5)$ QR code. In order to employ the BM algorithm to decode a code up to 2 errors, one needs in sequence the 4 syndromes, S_1, S_2, S_3, S_4. For the (17,9,5) code, the minimal distance is 5. It can correct up to 2 errors; however, the only syndromes that can be determined directly from $r(x)$ are S_1, S_2 and S_4. The syndrome S_3 is absent. It cannot be obtained by evaluating $r(x)$ at the roots of $g(x)$. The procedure given in [7], [20] to determine the unknown syndromes of this QR code is developed in the next subsection.

2.2. Efficient Algorithm to Determine the Unknown Syndromes

To develop the algorithm for determining the unknown syndromes, some extra notations are needed.

1. First let $I = \{i_1, i_2, \ldots, i_{v+1}\}$ denote a subset of $\{0, 1, \ldots, 46\}$ consisting of $v+1$ distinct elements.
2. Next, define a matrix $X(I)$ of size $(v+1) \times v$ as shown below:

$$X(I) = \begin{bmatrix} Z_1^{i_1} & Z_2^{i_1} & \ldots & Z_v^{i_1} \\ Z_1^{i_2} & Z_2^{i_2} & \ldots & Z_v^{i_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{i_v} & Z_1^{i_v} & \ldots & Z_1^{i_v} \\ Z_1^{i_{v+1}} & Z_1^{i_{v+1}} & \ldots & Z_1^{i_{v+1}} \end{bmatrix} \tag{8}$$

3. Also, let $J = \{j_1, j_2, \ldots, j_{v+1}\}$ be another $(v+1)$-subset of $\{0, 1, \ldots, 46\}$ and define a matrix $S(I, J)$ of size $(v+1) \times (v+1)$ as follows:

$$S(I, J) = X(I)X(J)^T,$$

where $X(J)^T$ denotes the transpose of the matrix $X(J)$.

In terms of this notation one has the following theorem describing the matrix $S(I, J)$.

Theorem 2.1. [13] The $(v+1) \times (v+1)$ matrix $S(I, J)$ in Eq. (7) has the form

$$S(I, J) = \begin{bmatrix} S_{i_1+j_1} & S_{i_1+j_2} & \ldots & S_{i_1+j_{v+1}} \\ S_{i_2+j_1} & S_{i_2+j_2} & \ldots & S_{i_2+j_{v+1}} \\ \vdots & \vdots & \ddots & \vdots \\ S_{i_v+j_1} & S_{i_v+j_2} & \ldots & S_{i_v+j_{v+1}} \\ S_{i_{v+1}+j_1} & S_{i_{v+1}+j_2} & \ldots & S_{i_{v+1}+j_{v+1}} \end{bmatrix} \tag{9}$$

where the summation of the sub-indices of the $S_i^{'s}$ are modulo 47. Moreover, the determinant of $S(I, J)$ equals zero, i.e.,

$$det(S(I, J)) = 0 \tag{10}$$

If the matrix $S(I, J)$ has unknown syndromes as its entries, then the equality $det(S(I, J)) = 0$ gives a polynomial equation for those unknown syndromes with coefficients that are functions of the known syndromes. If there is only one unknown syndrome, say S_r, among the entries of $S(I, J)$, then one can express S_r as a function in terms of known syndromes. Hence, during the decoding process, one is able to calculate the value of S_r with the information of such known syndromes. More precisely, one has the following theorem:

Theorem 2.2. [13] If among the entries of $S(I, J)$, there is only one unknown syndrome, say S_r, then S_r can be expressed as a fraction 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

$$S_r = \frac{det(\Delta_0)}{det(\Delta)}, \tag{11}$$

where Δ_0 is the $(v+1)' \times (v+1)$ matrix that is identical with $S(I, J)$ except for the (i, j)th entry which equals 0 instead of S_r, and Δ is the $v' \times v$ submatrix of $S(I, J)$, obtained by deleting the ith row and jth column of $S(I, J)$.

The proofs of theorems 2.1 and 2.2 are given in the Appendix [13]. Theorem 2.2 is used to determine the primary unknown syndrome S_3 of (17, 9, 5) QR code by searching for the two subsets I and J of $\{0, 1, \ldots, 16\}$ such that matrix $S(I, J)$ contains the unknown syndrome $_3$ as its entry only once. To do this, an exhaustive search needs at most $(C^{17}_{v+1})^2$ choices, where $(C^{17}_{v+1}) = (17!)/((17-(v+1))!(v+1)!)$ is the binomial coefficient for the number of combinations taking $v+1$ from a set of 17 elements. For the (17, 9, 5) QR code, the primary unknown syndrome is S_3. Let $Q = Q_{17}' \cup \{0, 3\}$. Before stating the algorithm, one needs some more notations. For $i' \in Q$, define the difference of i from Q to be:

$$Q - i = \{(q-i) \ mod \ 17 | q \in Q\}$$

.

Next, define a special sum of the two subsets I and J to be the multi-set; that is, each element should be kept, as $I \oplus J = \{(i+j) \ mod \ 17 | i' \in I, j' \in J\}^*$, where one uses a star-sign "' $*$ "' to indicate that the set is a multi-set.

For example, let $v = 1$ and $i = 1$. Then the difference of 1 from Q is

$$\begin{aligned} Q - 1 &= \{(q-1) \ mod \ 17 | q \in Q\} \\ &= \{0-1, 1-1, 2-1, \ldots, 16-1\} \\ &= \{16, 0, 1, 3, 7, 8, 12, 14, 15\}. \end{aligned}$$

Next, let $v = 2$, $I = \{1, 2\}$ and $J = \{0, 1\}$. Then

$$I \oplus J = \{1+0, 1+1, 2+0, 2+1\}^* = \{1, 2, 2, 3\}^*$$

.

With the above definitions the efficient algorithm to find the two $(v+1)$-subsets I, J, needed to determine the primary unknown syndrome S_r is as follows

Algorithm: [13]

Step 1: Choose a subset $I = \{i_1, i_2, ..., i_{v+1}\}' \subset Q$.

Step 2: Check the number of elements in the intersection $(Q - i_1)' \cap (Q - i_2)' \cap ... \cap$ $'(Q - i_{v+1})$. If this set intersection contains less than $v+1$ elements, return to step 1.

Step 3: Choose a subset J with $v+1$ elements from the intersection in step 2.

Step 4: Check the number of $r \notin Q_n$ in the multi-set $I \oplus J$. If the multi-set $I \oplus J$ contains exactly one r, then stop; I and J are the desired sets. Otherwise, return to step 3.

If the multi-set $I \oplus J$ contains exactly one r, then from Eq. (11), one can see that the matrix $S(I, J)$ has only one S_r as its entry, and all other entries belong to the set $Q_n{}' \cup \{0\}$. The proof of this algorithm can be found in the Appendix [13].

2.3. The Inverse Free Berlekamp-Massey Algorithm

To decode the (17, 9, 5) QR code, the inverse-free BM algorithm is much more efficient to implement than any other known algorithm, e.g. see [12]. A pseudo code for this inverse-free BM algorithm developed originally for BCH and RS codes is given below:

Step 1: Set initial values: $k = 1$, $C^{(0)}(x) = 1$, $A^{(0)}(x) = 1$, $\ell^{(0)} = 0$ and $\gamma^{(0)}$.

Step 2: Compute

$$\Delta^{(k)} = \sum_{j=0}^{\ell^{(k-1)}} c_j^{(k-1)} s_{k-j}, \tag{12}$$

where the coefficients $c^{(k-1)}$ are the coefficient of polynomial $C^{(k-1)}(x)$ at the $(k-1)$-th stage.

Step 3: Compute

$$C^{(k)}(x) = \gamma^{(k-1)} \cdot C^{(k-1)}(x) - \Delta^{(k)} A^{(k-1)}(x) \cdot x. \tag{13}$$

Step 4:

$$\begin{aligned} A^{(k)}(x) = x \cdot A^{(k-1)}(x) \quad & if\, \Delta^{(k)} = 0 \ \ or \ \ 2\ell^{(k-1)} > k-1 \\ C^{(k-1)}(x) \quad & if\, \Delta^{(k)} \neq 0 \ \ or \ \ 2\ell^{(k-1)} \leq k-1. \end{aligned} \tag{14}$$

$$\begin{aligned} \ell^{(k)} = \ell^{(k-1)} \quad & if\, \Delta^{(k)} = 0 \ \ or \ \ 2\ell^{(k-1)} > k-1 \\ k - \ell^{(k-1)} \quad & if\, \Delta^{(k)} \neq 0 \ \ or \ \ 2\ell^{(k-1)} \leq k-1 \end{aligned} \tag{15}$$

$$\begin{aligned} \gamma^{(0)} = \gamma^{(k-1)} \quad & if\, \Delta^{(k)} = 0 \ \ or \ \ 2\ell^{(k-1)} > k-1 \\ \Delta^{(k)} \quad & if\, \Delta^{(k)} \neq 0 \ \ or \ \ 2\ell^{(k-1)} \leq k-1 \end{aligned} \tag{16}$$

Step 5: set $k = k + 1$ if $k \leq 2t$, the step 2. Otherwise stop.

In the algorithm, the parameter t equals the maximum number of the errors that can be corrected, and $C^{(2t)}/c_0^{2t}$ denotes the error-locator polynomial $\sigma(z)$, defined in Eq. (13).

3. Proposed Algebraic Decoder for (17,9,5) QR Code using the IFBM Algorithm

This section is the main part of the paper. It illustrates the ideas needed to decode the (17, 9, 5) QR code. There are two subsections:

- The first subsection describes how to determine the primary unknown syndrome, S_3, for every case of a different number of errors,
- The second subsection shows how to use the inverse-free BM algorithm to find the error-locator polynomial from the sequence of the 4 known syndromes, including the one calculated unknown syndromes, for the (17, 9, 5) code.

Fig. 1 is a flowchart of the decoding method that consists of both the calculation of the unknown syndromes and the inverse-free BM algorithm. In this figure, for $r' \in \{3\}$, S_r^v denotes the unknown syndrome S_r for the v-errors case.

3.1. Determination of the Unknown Syndrome S_3

The three cases from case 0 to case 2 are discussed separately. The digit after the word "Case" indicates the number of errors for that case. In each case, one lists explicitly the two subsets I and J that are needed in Theorem 2 to determine the primary unknown syndrome S_3. Moreover, the attachment of a super-index to "S_5" to obtain the notation "$S_r^{(v)}$" indicates that it is valid for the v-error case only.

Case 0: (0 error) In this case where v=0, the Unknown Syndrome is $S_3^{(0)} = 0$.

Case 1: (1 error) Let us choose $I = \{0, 1\}$ and $J = \{1, 2\}$for $v = 1$
Then, by Theorem 2.1, one obtains the matrix $S(I_1, J_1)$ of size 2×2

$$S(I_1, J_1) = \begin{bmatrix} S_1 & S_2 \\ S_2 & S_3^{(1)} \end{bmatrix} \tag{17}$$

where $S_2 = S_1^2$. Thus, by Theorem 2, the unknown syndrome $S_3^{(1)}$ for 1-error case is given by

$$S_3^{(1)} = \frac{det(\Delta_0)}{det(\Delta)}.$$

where $\Delta = S_1$ and

$$\Delta_0 = \begin{bmatrix} S_1 & S_2 \\ S_2 & 0 \end{bmatrix}$$

This is a trival case : by defination of syndrome for 1- error case is $S_3^{(1)} = (Z_1)^3 = S_1^3$.

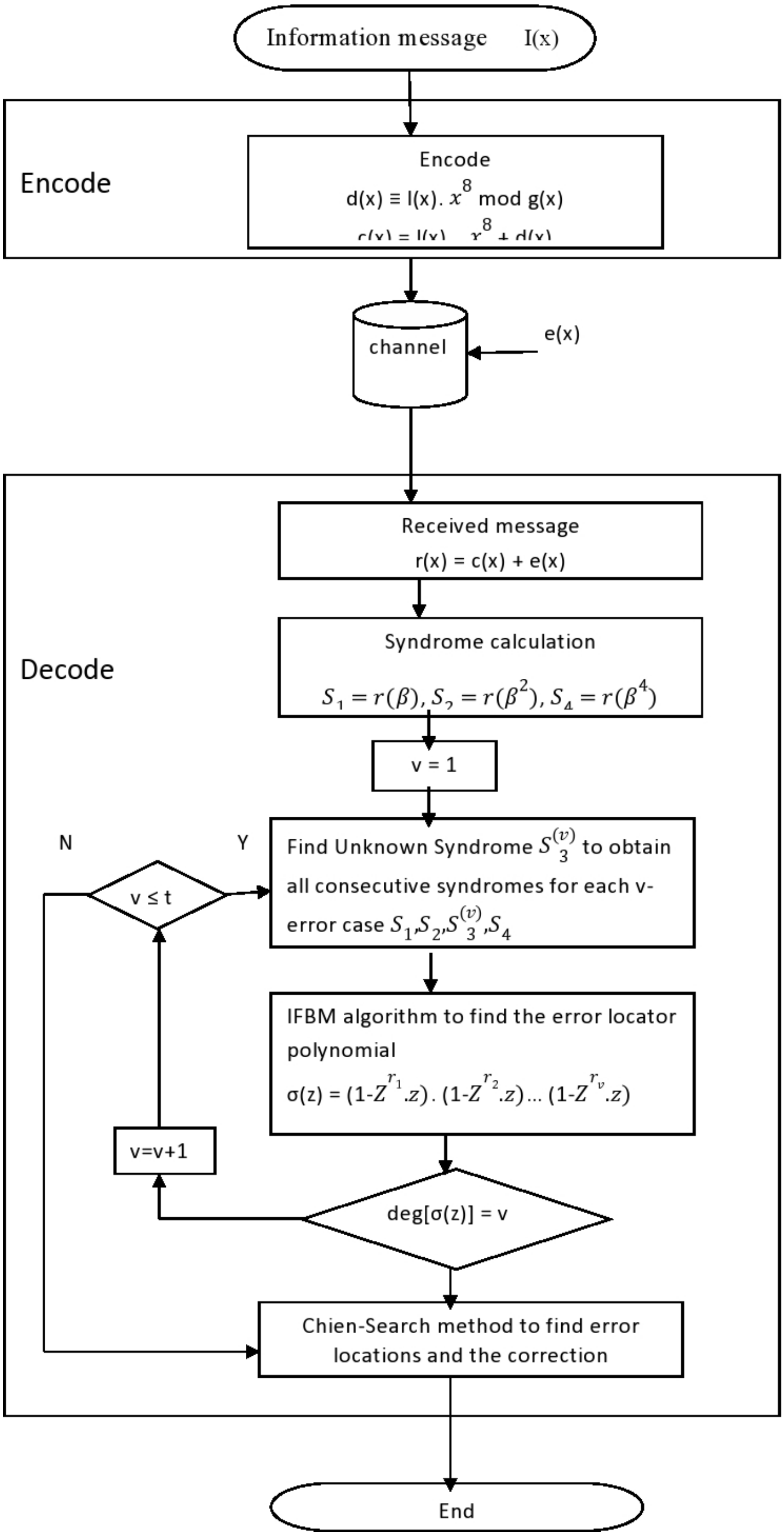
Information message I(x)
Encode
Encode
d(x) ≡ I(x). x^8 mod g(x)
c(x) = I(x) . x^8 + d(x)
channel
e(x)
Decode
Received message
r(x) = c(x) + e(x)
Syndrome calculation
$S_1 = r(\beta), S_2 = r(\beta^2), S_4 = r(\beta^4)$
v = 1
N
Y
v ≤ t
Find Unknown Syndrome $S_3^{(v)}$ to obtain all consecutive syndromes for each v-error case $S_1, S_2, S_3^{(v)}, S_4$
IFBM algorithm to find the error locator polynomial
σ(z) = (1-Z^{r_1}.z). (1-Z^{r_2}.z)… (1-Z^{r_v}.z)
v=v+1
deg[σ(z)] = v
Chien-Search method to find error locations and the correction
End

Figure 1: flowchart

case 2: (2 error) For $v = 2$, let us choose $I_2 = \{1, 13, 16\}$ and $J_2 = \{1, 4, 9\}$ Then, by Theorem 2.1, one obtains the matrix $S(I_2, J_2)$ of size 3×3

$$S(I_2, J_2) = \begin{bmatrix} S_1 & S_{13} & S_{16} \\ S_5 & S_3^{(2)} & S_1 \\ S_0 & S_4 & S_8 \end{bmatrix} \tag{18}$$

where $S_0 = 0, S_4 = S_1^4, S_5 = S_1^{32}, S_8 = S_1^8, S_{13} = S_1^{64}, S_{16} = S_1^{16}$. Thus, by Theorem 2.2, the unknown syndrome $S_3^{(2)}$ for 2-error case is given by

$$S_3^{(2)} = \frac{det(\Delta_0)}{det(\Delta)}$$

. where

$$\Delta = \begin{bmatrix} S_1 & S_{16} \\ S_0 & S_8 \end{bmatrix}$$

and

$$\Delta_0 = \begin{bmatrix} S_1 & S_{13} & S_{16} \\ S_5 & 0 & S_1 \\ S_0 & S_4 & S_8 \end{bmatrix}$$

To illustrate this algorithm, let us consider details of this simple example of a QR code are given here of the (17, 9, 5) QR code.

3.2. Example

To decode the (17, 9, 5) QR code, first, let S_k^v denote the unknown syndrome which is computed from v errors that occur in the received vector, where $k' \in 1, 2, 3, 4$ and $v' \in 1, 2,$. Then one can construct the needed consecutive syndromes S_1, S_2, S_3^v, S_4 for the inverse-free BM algorithm. Let $\beta = \alpha^{15}$ be a primitive $17 - th$ root of unity in $GF(2^8)$, where α is a root of the primitive polynomial $P(x) = x^8 + x^4 + x^3 + x^2 + 1$ The set of quadratic residues modulo is $Q_{17} = \{1, 2, 4, 8, 9, 13, 15, 16\}$. The generator polynomial of the (23, 12, 7) QR code is given by

$$g(x) = \prod_{i \in Q_{17}} (x - \beta_i) = x^8 + x^5 + x^4 + x^3 + 1$$

Let be the $I = (0, 0, 1, 1, 0, 1, 0, 0, 1)$ message. Multiplying its associated polynomial

$$I(x) = x^6 + x^5 + x^3 + 1 \text{ by } g(x),$$

one obtains the code polynomial

$$c(x) = I(x) \cdot x^8 + d(x) = x^{14} + x^{13} + x^{11} + x^9 + x^7 + x^6 + x^3 + 1,$$

where $d(x)$ is the reminder of $I(x) \cdot x_8$ divided by g(x).
Let c be the code vector of this polynomial $c = (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 1)$

Let us assume that there will be one error in the message and the error vector $\mathbf{e} = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1)$. Then the received vector is

$$r = c + e = (0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0, 0)$$

and its associated polynomial is

$$r(x) = x^{14} + x^{13} + x^{11} + x^9 + x^7 + x^6 + x^3.$$

For $i = 1{,}2$ and 4, the syndromes are

$$S_i = r(\beta^i) = (\beta^i)^{14} + (\beta^i)^{13} + (\beta^i)^{11} + (\beta^i)^9 + (\beta^i)^6 + (\beta^i)^3 + 1.$$

That is ,$S_1 = \alpha^{15}$, $S_2 = \alpha^{30}$, and$S_4 = \alpha^{60}$.

By the use of Eqs. (17) and (11),the single un-known syndrome for 1- error case is found to be $S_3 = \alpha^{45}$. Using the inverse-free BM algorithm, the computation terminates at step $k = 4$, and one obtains

$$C^{(4)} = \alpha^{60}x + \alpha^{45}$$

from the consecutive syndromes $S_1 = \alpha^{15}$, $S_2 = \alpha^{30}$, $S_3 = \alpha^{45}$, and $S_4 = \alpha^{60}$. In the last step, $deg[C^{(6)}] = 1 = v$ so that

$$\begin{aligned} C^{(4)}(z) &= (1 + \sigma_1 z).\sigma_0 \\ &= (1 + \alpha^{15} z).\alpha^{45} \\ &= (1 + Z_1 z).\alpha^{45}. \end{aligned}$$

The root of $\sigma(z)$ is $Z_1 = \alpha^{-15} = \beta^{-1}$. Thus, the error polynomial is $e(x) = x^1$

As in the above illustrative example of the (17, 9, 5) QR code the decoder This algorithm is summarized by the following seven steps:

1. Initialize by letting $v = 1$.
2. Compute the known syndromes S_1, S_2, S_4, from Eq. (3).
3. Compute the two unknown syndromes S_3^v for $1 \le v \le 5$ from the algorithm developed in section 3.1
4. Compute the error-locator polynomial $\sigma(z)$ from the consecutive known syndromes S_1, S_2, S_3^v, S_4 for v errors, using the inverse-free BM algorithm.
5. If $deg[\sigma(z)] = v$ go to step (7). Otherwise set $v = v + 1$.

6. If $v > t$, stop. Otherwise, go to step (3).

7. Obtain the error-locator polynomial $\sigma(z)$ with $deg[\sigma(z)] = v$ for the v-errors case, and compute the roots of $\sigma(z)$ by a use of the Chien-search method. Finally, the corrected QR code is obtained by subtracting the error vector from the received vector.

4. Conclusion

The generally utilized BM calculation was initially created to interpret both BCH and RS codes. It is the most powerful and efficient method for determining the error-locator polynomial of a code. The primary condition needed to be able to apply the BM algorithm is that it has enough consecutive syndromes. Unfortunately, the QR codes do not have enough consecutive syndromes to entirely decode all errors; some syndromes are missing. In this paper it is shown how to find the unknown syndromes to provide the absent terms. As a consequence, the completed syndrome list is obtained for the inverse-free BM algorithm. Also an efficient algorithm is found to calculate the desired unknown syndromes.

Although these algorithms are designed for the (17, 9, 5) QR code and can be extended to every QR code with irreducible generating polynomial, In this paper, the result shows for the (17, 9, 5) QR code to correct all cases of 2 or less errors without mistake. This algorithm is easier to implement for both software and the hardware design, compared with the decoding algorithm for the (17, 9, 5) QR code found in [19] previously by part of the authors of the present paper.

References

[1] E. Prange, "Cyclic error-correcting codes in two symbols," AFCRC-TN-57-103, Air Force Cambridge Research Center, Cambridge, Mass. September 1957.

[2] S. B. Wicker, Error Control Systems for Digital Communication and Storage, Englewood Cliffs, NJ: Prentice Hall, 1995.

[3] M. Elia, "Algebraic decoding of the (23, 12, 7) Golay codes," IEEE Trans. Inf. Theory, vol. 33, no. 1, pp. 150–151, January 1987.

[4] I. S. Reed, X. Yin, T. K. Truong, and J. K. Holmes, "Decoding the (24,12, 8) Golay code," Proc. IEE, vol. 137, no. 3, pp. 202–206, May 1990.

[5] I. S. Reed, X. Yin, and T. K. Truong, "Algebraic decoding of the (32, 16,8) quadratic residue code," IEEE Trans. Inf. Theory, vol. 36, no. 4, pp. 876–880, July 1990.

[6] I. S. Reed, T. K. Truong, X. Chen, X. Yin, "The algebraic decoding of the (41, 21, 9) Quadratic Residue code," IEEE Trans. Inf. Theory, vol. 38, no. 3, pp. 974–986, May 1992.

[7] R. He, I. S. Reed, T. K. Truong, and X. Chen, "Decoding the (47, 24, 11) quadratic residue code," IEEE Trans. Inf. Theory, vol. 47, no. 3, pp. 1181–1186, March 2001.

[8] T. C. Lin, T. K. Truong, H. P. Lee, and H. C. Chang, "Algebraic decoding of the (41, 21, 9) Quadratic Residue code," Inf. Sci., vol. 179, no. 19, pp. 3451–3459, September 2009.

[9] T. C. Lin, H. C. Chang, H. P. Lee, S. I. Chu, and T. K. Truong, "Decoding of the (31, 16, 7) Quadratic Residue code," J. Chin. Inst. Eng., vol. 33, no. 4, pp. 573–580, June 2010.

[10] X. Chen, I. S. Reed, T. Helleseth, T. K. Truong, "Use of Grobner bases to decode binary cyclic codes up to the true minimum distance," IEEE Trans. on Comm., vol. 40, no. 5, pp. 1654–1661, September. 1994.

[11] 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," Inf. Sci., vol. 180, no. 20, pp. 4060–4068, October 2010.

[12] I. S. Reed, M. T. Shih, and T. K. Truong, "VLSI design of inverse-free Berlekamp-Massey algorithm," IEE Proc. On Computers and Digital Techniques, vol. 138, no. 5, pp. 295–298, September 1991.

[13] Y. H. Chen, T. K. Truong, Y. Chang, C. D. Lee, and S.H. Chen, "Algebraic Decoding of Quadratic Residue Codes Using BerlekampMassey Algorithm," J. Inf. Sci. Eng., vol. 23, no. 1, January 2007

[14] Y. Chang, T. K. Truong, I. S. 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 Trans. on Comm., vol. 51, no. 9, pp. 1463–1473, September 2003.

[15] T. K Truong, P. Y. Shih, W. K. Su, C. D. Lee, and Y Chang, "Algebraic Decoding of The (89, 45, 17) Quadratic Residue Code," IEEE Trans. Inf. Theory, vol. 54, no. 11, pp. 5005–5011, November 2008.

[16] Y. Chang , C. D. Lee, "Algebraic decoding of a class of binary cyclic codes via Lagrange interpolation formula," IEEE Trans. Inf. Theory, v.56 n.1, p. 130–139, January 2010.

[17] R. T. Chien, "Cyclic decoding procedure for the Bose-ChaudhuriHocquenghem codes," IEEE Trans. on Inf. Theory, vol. 10, no. 4, pp. 357–363, October 1964.

[18] C. C. Wang, T. K. Truong, H. M. Shao, L. J. Deutsch, J. K. Omura, and I. S. Reed, "VLSI Architectures for Computing Multiplications and Inverses in GF(2m)," IEEE Transactions on Computers., vol. C-34, no. 8, pp. 709–716, Auguest 1985.

[19] H. P. Lee, "Fast algebraic decoding of the (17, 9, 5) quadratic residue code", 2012, 2nd International Conference on 2012.

[20] I. M. Duursma and R. Kotter. "Error-locating pairs for cyclic codes", IEEE Trans. on Inf. Theory, vol. IT-40, 1994, pp. 1108–1121,