International Journal of Networks and Communications 2013, 3(2): 39-44
DOI: 10.5923/j.ijnc.20130302.01

Analysis on the Algebraic Decoding of the (31, 16, 7) QR Code by Using IFBM Algorithm

Hung-Peng Lee

Department of Computer Science and Information Engineering, Fortune Institute of Technology, Kaohsiung, 83160, Taiwan

Abstract An analysis on the algebraic decoding of the (31, 16, 7) quadratic residue (QR) code with reducible generator polynomial that uses the inverse-free Berlekamp-Massey (IFBM) algorithm to determine the error-locator polynomial is presented in this paper. The primary known syndrome S_1 will be equal to zero for some weight-3 error patterns. However, the zero S_1 does not cause a decoding failure while using the IFBM algorithm to determine the error-locator polynomial. Two examples with detailed step-by-step analysis show the decoding procedure.

Keywords Quadratic Residue Code, Algebraic Decoding Algorithm, Inverse-Free Berlekamp-Massey Algorithm, Error Pattern, Syndrome

1. Introduction

The well-known QR codes, introduced by Prange[1] in 1957, are cyclic BCH codes with code rates greater than or equal to one-half. In addition, the codes generally have large minimum distances so that most of the known QR codes are the best-known codes. The code augmented by a parity bit, for example, the (24, 12, 8) QR code was utilized to provide error control on the Voyager deep-space mission[2].

In the past decades, several decoding techniques have been developed to decode the binary QR codes. The ADAs most used to decode the QR codes are the Newton identities with either Sylvester resultants[3-7,12-13,15] or Gröbner bases[16] , or inverse-free Berlekamp-Massey (IFBM) algorithm[8-11,14] to determine the error-locator polynomial. Among them, the ADA of the (31, 16, 7) QR code[5,12,14,15] with the reducible polynomial can correct up to three errors in the finite field GF(2^5), because the error-correcting capability of the code is $t = \lfloor (d-1)/2 \rfloor = \lfloor (7-1)/2 \rfloor = 3$ errors, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x, and $d = 7$ is the minimum Hamming distance of the code. In[5,12,15], the Newton identities are applied to determine the coefficients of the error-locator polynomials. In[14], the IFBM algorithm[18] is applied to determine the error-locator polynomial of the received sequence. Finally, the Chien search algorithm[19] is applied to find the roots of the error-locator polynomial.

In[15], the decoding algorithm is very complicated because the syndrome $S_7 = 0$. However, the IFBM does not use the syndrome S_7 to determine the error-locator polynomial of the (31, 16, 7) QR code. For the QR codes with irreducible generator polynomial, the primary known syndrome S_1 cannot be equal to zero, because the zero S_1 denotes that the received word has no errors in the transmission channel. Besides, $S_1 = 0$ means that the power (mod codelength n) of S_1 are all zero; that is, $S_2 = (S_1)^2 = 0$, $S_4 = (S_1)^4 = 0$, …. For the (89, 45, 17) QR code with reducible generator polynomial in the finite field GF(2^{11}), the IFBM algorithm can be used to determine the error-locator polynomial while the syndrome $S_1 = 0$[20]. Similarly, for the (31, 16, 7) QR code with reducible generator polynomial in the finite field GF(2^5), the zero primary known syndromes, $S_1 = 0$ and $S_5 = 0$, do not cause a decoding failure in decoding weight-3 error patterns while using the IFBM algorithm to determine the error-locator polynomial. The analysis of two examples on the weight-3 error patterns shows the fact.

The rest parts of this paper are organized as follows: The background of systematic (31, 16, 7) QR codes is briefly given in Section 2. The analysis on the zero primary known syndromes for the weight-3 error patterns is presented in Section 3. Finally, this paper concludes with a brief summary in Section 4.

2. Background of the Binary (31, 16, 7) QR Code

The codeword of the binary (n, k, d) QR code is defined algebraically as a multiple of its generator polynomial $g(x)$ with coefficients in GF(2). Let the length of the code 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 $2^m \equiv 1$ (mod n). Thus, GF(2^m) is the extension field of GF(2). Also, let $k = (n+1)/2$ be the message length and d be the minimum

* Corresponding author: Hung-Peng Lee
hpl@center.fotech.edu.tw (Hung-Peng Lee)
Published online at http://journal.sapub.org/ijnc

Hamming distance or Hamming weight of the code. The generator polynomial as a cyclic code is given by

$$g(x) = \prod_{i \in Q_n} (x - \beta^i), \quad (1)$$

where the element β is a primitive nth root of unity in GF(2^m) and Q_n denotes the set of quadratic residues given by Q_n = $\{j | j \equiv x^2 \bmod n$ for $1 \le x \le (n-1)/2\}$. The set Q_n can thus be represented as a disjoint union of cyclotomic cosets, modulo n. These cyclotomic cosets are defined as $Q_r = \{r2^j | j = 0, 1, \ldots, n_r - 1\}$, where n_r is the smallest positive integer such that $r2^{n_r} \equiv r \bmod n$, n_r divides $(n-1)/2$, and r is the smallest element in Q_r. The element r is called the representative element of the cyclotomic cosets Q_r. The set S, consisting of all representatives of the QR code, is called the base set of the QR code. These definitions and properties cause the equality $Q_n = \bigcup_{r \in S} Q_r$ relating Q_n to the cyclotomic cosets, modulo n.

Let an element $\alpha \in$ GF(2^5) be a root of the primitive polynomial $p(x) = x^5 + x^2 + 1$. Then, α generates the multiplicative group of nonzero elements in GF(2^5). Also, let an element $\beta = \alpha^u$, where $u = (2^m - 1)/n = (2^5 - 1)/31 = 1$, is a primitive 31th root of unity in GF(2^5); that is, $\beta = \alpha$. The all 31 roots of $x^{31} - 1 = 0$ are shown in Table 1.

Table 1. The 31 Roots of $x^{31} - 1 = 0$

Exponential representation	Polynomial representation	Exponential representation	Polynomial representation
α	α	α^2	α^2
α^3	α^3	α^4	α^4
α^5	$\alpha^2 + 1$	α^6	$\alpha^3 + \alpha$
α^7	$\alpha^4 + \alpha^2$	α^8	$\alpha^3 + \alpha^2 + 1$
α^9	$\alpha^4 + \alpha^3 + \alpha$	α^{10}	$\alpha^4 + 1$
α^{11}	$\alpha^2 + \alpha + 1$	α^{12}	$\alpha^3 + \alpha^2 + \alpha$
α^{13}	$\alpha^4 + \alpha^3 + \alpha^2$	α^{14}	$\alpha^4 + \alpha^3 + \alpha^2 + 1$
α^{15}	$\alpha^4+\alpha^3+\alpha^2+\alpha+1$	α^{16}	$\alpha^4 + \alpha^3 + \alpha + 1$
α^{17}	$\alpha^4 + \alpha + 1$	α^{18}	$\alpha + 1$
α^{19}	$\alpha^2 + \alpha$	α^{20}	$\alpha^3 + \alpha^2$
α^{21}	$\alpha^4 + \alpha^3$	α^{22}	$\alpha^4 + \alpha^2 + 1$
α^{23}	$\alpha^3 + \alpha^2 + \alpha + 1$	α^{24}	$\alpha^4 + \alpha^3 + \alpha^2 + \alpha$
α^{25}	$\alpha^4 + \alpha^3 + 1$	α^{26}	$\alpha^4 + \alpha^2 + \alpha + 1$
α^{27}	$\alpha^3 + \alpha + 1$	α^{28}	$\alpha^4 + \alpha^2 + \alpha$
α^{29}	$\alpha^3 + 1$	α^{30}	$\alpha^4 + \alpha$

The base set of this code is $S = \{1, 5, 7, 3, 11, 15\}$ and $r \in S$. The minimal polynomial $g_r(x)$ can also be expressed as $g_r(x) = \prod_{i=0}^{4} (x - \beta^{2^i r})$. Therefore, the six cyclotomic cosets Q_r and their corresponding minimal polynomials are shown in Table 2.

Table 2. The Cyclotomic Cosets of the (31, 16, 7) QR Code

r	Q_r,	$g_r(x)$
1	{1,2,4,8,16}	$x^5 + x^2 + 1$
5	{5,10,20,9,18}	$x^5 + x^4 + x^2 + x + 1$
7	{7,14,28,25,19}	$x^5 + x^3 + x^2 + x + 1$
3	{3,6,12,24,17}	$x^5 + x^4 + x^3 + x^2 + 1$
11	{11,22,13,26,21}	$x^5 + x^4 + x^3 + x + 1$
15	{15,30,29,27,23}	$x^5 + x^3 + 1$

Let r = 1, 5, and 7, respectively, the quadratic residue set of the code is

$$\begin{aligned} Q_{31} &= Q_1 \cup Q_5 \cup Q_7 \\ &= \{1,2,4,8,16,5,10,20,9,18,7,14,28,25,19\}. \end{aligned} \quad (2)$$

Thus, the $g(x)$ consists of the following three minimum polynomials:

$$\begin{aligned} g(x) &= \prod_{i \in Q_{31}} (x - \beta^i) \\ &= g_1(x) g_5(x) g_7(x) \\ &= x^{15} + x^{14} + x^{13} + x^9 + x^8 + x^3 + 1 . \end{aligned} \quad (3)$$

Since the codewords are a multiple of the $g(x)$, the codeword polynomial of the (31, 16, 7) QR code can be represented by $c(x) = \sum_{i=0}^{30} c_i x^i = m(x) g(x)$, where $c_i \in$ GF(2) for $0 \le i \le 30$, and $m(x) = m_{15}x^{15} + \cdots + m_1 x + m_0$ denotes information polynomial, where $m_i \in$ GF(2) for $0 \le i \le 15$. In such a representation, this type of codeword is called the non-systematic encoding. In practice, the encoding procedure is often implemented by the use of systematic encoding. Let $p(x) = p_{14}x^{14} + \cdots + p_1 x + p_0$ be the parity-check polynomial, where $p_i \in$ GF(2) for $0 \le i \le 14$. Also, let $m(x)x^{n-k}$ divide by $g(x)$, then we get the following identity:

$$m(x)x^{n-k} = q(x)g(x) + d(x). \quad (4)$$

Multiplying both sides of (4) 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.

$$c(x) = d(x)x^k + m(x) = p(x) + m(x). \quad (5)$$

As shown in (5), 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 $e(x) = e_{30}x^{30} + \cdots + e_1 x + e_0$ 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 $\mathbf{c} = (c_{30}, \ldots, c_1, c_0)$. The syndromes or known syndromes of the code are defined by

$$S_i = r(\beta^i) = e(\beta^i) = \sum_{j=0}^{30} e_j (\beta^i)^j, \quad (6)$$

where $i \pmod{31} \in Q_{31}$. If $i \notin Q_{31}$, the syndromes are called unknown syndromes. All known and unknown syndromes can be expressed as some powers of S_1, S_5, S_7, and S_3, S_{11}, S_{15}, called the primary known syndromes and the primary unknown syndromes, respectively. For example, $S_2 = S_1^2$, $S_4 = S_1^4$, $S_8 = S_1^8$, and $S_{16} = S_1^{16}$. 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 $1 \le v \le 3$.

If there are $v \le t$ errors in $r(x)$, then $e(x)$ has v nonzero terms over GF(2); that is, $e(x) = x^{r_1} + x^{r_2} + \cdots + x^{r_v}$, where $0 \le r_1 < r_2 < \ldots < r_v \le n-1$. For $i \in Q_n$, the syndrome can be written as $S_i = X_1^i + X_2^i + \cdots + X_v^i$, where $X_j = \beta^{r_j}$ for $1 \le j \le v$ are called the error locators. Assuming that v errors

occur, the classical error-locator polynomial $L(x)$ is defined by

$$L(x) = \prod_{j=1}^{v}(1 - X_j x) = \sigma_v x^v + \cdots + \sigma_1 x + \sigma_0 , \quad (7)$$

where the σ_j are called the elementary symmetric functions for $1 \le j \le v$ and $\sigma_0 = 1$. The roots of $L(x)$ are the inverse of the v error locators $\{X_j\}$.

The steps of the IFBM algorithm are summarized as below:

1). Initialize $k = 0$, $\mu^{(0)}(x) = 1$, $\lambda^{(0)}(x)=1$, $l^{(0)} = 0$, $\gamma^{(0)} = 1$.

2). Compute

$$\delta^{(k)} = \sum_{j=0}^{l^{(k-1)}} \mu_j^{(k-1)} S_{k-j} , \quad (8)$$

where $\mu_j^{(k-1)}$ is the coefficient of $\mu^{(k-1)}(x)$.

3). Compute

$$\mu^{(k)}(x) = \gamma^{(k-1)}\mu^{(k-1)}(x) - \delta^{(k)}\lambda^{(k-1)}(x)x. \quad (9)$$

4). Compute

$$\lambda^{(k)}(x) = \begin{cases} x\lambda^{(k-1)}(x), \text{ if } \delta^{(k)} = 0 \text{ or } 2l^{(k-1)} > k-1 \\ \mu^{(k-1)}(x), \text{ if } \delta^{(k)} \neq 0 \text{ and } 2l^{(k-1)} \le k-1 \end{cases}$$

$$l^{(k)} = \begin{cases} l^{(k-1)}, \text{ if } \delta^{(k)} = 0 \text{ or } 2l^{(k-1)} > k-1 \\ k - l^{(k-1)}, \text{ if } \delta^{(k)} \neq 0 \text{ and } 2l^{(k-1)} \le k-1 \end{cases} \quad (10)$$

$$\gamma^{(k)} = \begin{cases} \gamma^{(k-1)}, \text{ if } \delta^{(k)} = 0 \text{ or } 2l^{(k-1)} > k-1 \\ \delta^{(k)}, \text{ if } \delta^{(k)} \neq 0 \text{ and } 2l^{(k-1)} \le k-1 \end{cases}$$

5). Set $k = k + 1$. If $k \le 2t$, then go to step 2. Otherwise go to stop and declare a decoding failure.

3. Analysis on the Zero Primary Known Syndromes for the Weight-3 Error Patterns

The ADA given in[14] used the IFBM algorithm to determine the error-locator polynomial. In order to use the IFBM algorithm, the consecutive syndromes, Si for $1 \le i \le 6$, need to be computed first. Among them, there are two unknown syndromes S3, and S6, where S6 can be computed from the square of S3. The determination of the unknown syndrome S3 is computed from (17) of[12].

For the (31, 16, 7) QR code, a C++ program shows that there are 155 weight-3 error patterns will cause the primary known syndromes and the primary unknown syndromes to be equal to zero; however, they are not simultaneous equal to zero. The zero primary known syndromes do not cause a decoding failure while using the IFBM algorithm to determine the error-locator polynomial. The following example shows the decoding procedure.

3.1. The Case of Primary Known Syndrome $S_1 = 0$

Example 1:

If $m(x) = x^7$, by (4) and (5), then the systematic codeword is $c(x) = x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{20} + x^{19} + x^7$. If there is a weight-3 error pattern $e(x) = x^{18} + x + 1$ occurred in the transmission channel, then the received word becomes $r(x) = x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{20} + x^{19} + x^{18} + x^7 + x + 1$.

The syndromes $S_1 = 0$, $S_2 = 0$, $S_4 = 0$, and $S_5 = \alpha^{30}$ are computed by (6), respectively, and the syndromes $S_3 = \alpha^{19}$ and $S_6 = S_3^2 = \alpha^7$ are computed by (17) in[12]. Next, the IFBM algorithm is applied to obtain the error-locator polynomial. The decoding procedure is described as follows:

Define initial value as follows: $k = 0$, $\mu^{(0)}(x) = 1$, $\lambda^{(0)}(x)=1$, $l^{(0)} = 0$, $\gamma^{(0)} = 1$.

Set $k = k + 1 = 0 + 1 = 1$. By (8), compute $\delta^{(1)} = \sum_{j=0}^{l^{(0)}=0} \mu_j^{(0)} S_{1-j} = \mu_0^{(0)} S_1 = 0$.

By (9), compute $\mu^{(1)}(x) = \gamma^{(0)}\mu^{(0)}(x) - \delta^{(1)}\lambda^{(0)}(x)\cdot x = 1\cdot 1 - 0\cdot 1\cdot x = 1$.

The condition in (10) is $\delta^{(1)} = 0$. Compute $\lambda^{(1)}(x) = x\lambda^{(0)}(x) = x$, $l^{(1)} = l^{(0)} = 0$, and $\gamma^{(1)} = \gamma^{(0)} = 1$, respectively. Go to step 2.

Set $k = k + 1 = 1 + 1 = 2$. By (8), compute $\delta^{(2)} = \sum_{j=0}^{l^{(1)}=0} \mu_j^{(1)} S_{2-j} = \mu_0^{(1)} S_2 = 0$.

By (9), compute $\mu^{(2)}(x) = \gamma^{(1)}\mu^{(1)}(x) - \delta^{(2)}\lambda^{(1)}(x)x = 0\cdot 1 - 0\cdot 1\cdot x = 1$.

The condition in (10) is $\delta^{(2)} = 0$. Compute $\lambda^{(2)}(x) = x\lambda^{(1)}(x) = xx = x^2$, $l^{(2)} = l^{(1)} = 0$, and $\gamma^{(2)} = \gamma^{(1)} = 1$, respectively. Go to step 2.

Set $k = k + 1 = 2 + 1 = 3$. By (8), compute $\delta^{(3)} = \sum_{j=0}^{l^{(2)}=0} \mu_j^{(2)} S_{3-j} = \mu_0^{(2)} S_3 = 1S_3 = S_3$.

By (9), compute $\mu^{(3)}(x) = \gamma^{(2)}\mu^{(2)}(x) - \delta^{(3)}\lambda^{(2)}(x)\cdot x = 1\cdot 1 - S_3\cdot x^2\cdot x = 1 + S_3 x^3$.

The conditions in (10) are $\delta^{(3)} = S_3 \neq 0$ and $2l^{(2)} = 0 \le k - 1 = 3 - 1 = 2$. Compute $\lambda^{(3)}(x) = \mu^{(2)}(x) = 1$, $l^{(3)} = k - l^{(2)} = 3 - 0 = 3$, and $\gamma^{(3)} = \delta^{(3)} = S_3$, respectively. Go to step 2.

Set $k = k + 1 = 3 + 1 = 4$. By (8), compute.

$$\delta^{(4)} = \sum_{j=0}^{l^{(3)}=3} \mu_j^{(3)} S_{4-j} = \mu_0^{(3)} S_4 + \mu_1^{(3)} S_3 + \mu_2^{(3)} S_2 + \mu_2^{(3)} S_1 = 0.$$

By (9), compute $\mu^{(4)}(x) = \gamma^{(3)}\mu^{(3)}(x) - \delta^{(4)}\lambda^{(3)}(x)\cdot x = S_3(1 - S_3 x^3) = S_3 + S_3^2 x^3$.

The condition in (10) is $\delta^{(4)} = 0$. Compute $\lambda^{(4)}(x) = x\cdot 1 = x$, $l^{(4)} = l^{(3)} = 3$, and $\gamma^{(4)} = \gamma^{(3)} = S_3$, respectively. Go to step 2.

Set $k = k + 1 = 4 + 1 = 5$. By (8), compute $\delta^{(5)} = \sum_{j=0}^{l^{(4)}=3} \mu_j^{(4)} S_{5-j} = S_3 S_5 + 0S_4 + 0S_3 + S_3^2 S_2 = S_3 S_5$.

By (9), compute the error-locator polynomial of degree 3, $\mu^{(5)}(x) = \gamma^{(4)}\mu^{(4)}(x) - \delta^{(5)}\lambda^{(4)}(x)\cdot x = S_3(S_3 + S_3^2 x^3) - (S_3 S_5)xx = S_3^2 + S_3 S_5 x^2 + S_3^3 x^3$.

The condition in (10) is $2l^{(k-1)} = 2l^{(4)} = 6 > k - 1 = 5 - 1 = 4$. Compute $\lambda^{(5)}(x) = x\lambda^{(4)}(x) = xx = x^2$, $l^{(5)} = l^{(4)} = 3$, and $\gamma^{(5)} = \gamma^{(4)} = S_3$, respectively. Go to step 2.

Set $k = k + 1 = 5 + 1 = 6$. By (8), compute $\delta^{(6)} = \sum_{j=0}^{l^{(5)}=3} \mu_j^{(5)} S_{6-j} = S_3^2 S_6 + 0S_5 + S_3 S_5 S_4 + S_3^3 S_3 = 0$.

By (9), compute the error-locator polynomial of degree 3, $\mu^{(6)}(x) = \gamma^{(5)}\mu^{(5)}(x) - \delta^{(6)}\lambda^{(5)}(x)x = S_3(S_3^2 + S_3 S_5 x^2 + S_3^3 x^3) = S_3^3 + S_3^2 S_5 x^2 + S_3^4 x^3$.

The condition in (10) is $\delta^{(6)} = 0$, compute $\lambda^{(6)}(x) = x\lambda^{(5)}(x) = xx^2 = x^3$, $l^{(6)} = l^{(5)} = 3$, and $\gamma^{(6)} = \gamma^{(5)} = S_3$, respectively. Go to step 2.

Set $k = k + 1 = 6 + 1 = 7$. Since $k = 7 > 2t = 6$, go to stop.

The above decoding procedure is simplified in Table 3.

Table 3. The Simplified Decoding Procedure for Example 1

k	$\mu^{(k)}(x)$	$\lambda^{(k)}(x)$	$l^{(k)}$	$\gamma^{(k)}$	$\delta^{(k)}$
0	1	1	0	1	-
1	1	x	0	1	0
2	1	x^2	0	1	0
3	$1 + S_3x^3$	1	3	S_3	S_3
4	$S_3 + S_3^2x^3$	x	3	S_3	0
5	$S_3^2 + S_3S_5x^2 + S_3^3x^3$	x^2	3	S_3	S_3S_5
6	$S_3^3 + S_3^2S_5x^2 + S_3^4x^3$	x^3	3	S_3	0
7	Stop				

When $k = 6$, one obtains the error-locator polynomial $\mu^{(6)}(x) = L(x) = S_3^3 - S_3^2S_5x^2 - S_3^4x^3$, which means that $\mu^{(6)}(x)$ has three roots. By applying Chien search algorithm, the roots of $L(x)$ are exactly the inverse of the three error locators {0, 1, 18}. For example, the third error locator is α^{18}, and the reciprocal of α^{18} is α^{13}. Substituting α^{13} into $L(x)$, then the error-locator polynomial $L(\alpha^{13}) = S_3^3 + S_3^2S_5(\alpha^{13})^2 + S_3^4(\alpha^{13})^3 = (\alpha^{19})^3 + (\alpha^{19})^2(\alpha^{30})(\alpha^{13})^2 + (\alpha^{19})^4(\alpha^{13})^3 = \alpha^{26} + \alpha + \alpha^{22} = 0$. Similarly, the first and the second error locators are α^0 and α^1, then we obtain $L(1) = 0$ and $L(\alpha^{30}) = 0$, respectively. A C++ program shows that the total 155 weight-3 error patterns with $S_1 = 0$ can be corrected.

3.2. The Case of Primary Known Syndrome $S_5 = 0$

Example 2:

If $m(x) = x^7$, by (4) and (5), then the systematic codeword is $c(x) = x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{20} + x^{19} + x^7$. If there is a weight-3 error pattern $e(x) = x^{19} + x + 1$ occurred in the transmission channel, then the received word becomes $r(x) = x^{30} + x^{29} + x^{27} + x^{26} + x^{25} + x^{20} + x^7 + x + 1$.

The known syndromes $S_1 = \alpha^5$, $S_2 = \alpha^{10}$, $S_4 = \alpha^{20}$, and $S_5 = 0$ are computed by (6), respectively, and the known syndromes $S_3 = \alpha^{24}$ and $S_6 = \alpha^{17}$ are computed by (17) in[12]. Next, the IFBM algorithm is applied to obtain the error-locator polynomial. The decoding procedure is described as follows:

Define initial value as follows: $k = 0$, $\mu^{(0)}(x) = 1$, $\lambda^{(0)}(x)=1$, $l^{(0)} = 0$, $\gamma^{(0)} = 1$.

Set $k = k + 1 = 0 + 1 = 1$. By (8), compute $\delta^{(1)} = \sum_{j=0}^{l^{(0)}=0} \mu_j^{(0)} S_{1-j} = \mu_0^{(0)} S_1 = S_1$.

By (9), compute $\mu^{(1)}(x) = \gamma^{(0)}\mu^{(0)}(x) - \delta^{(1)}\lambda^{(0)}(x)\cdot x = 1\cdot 1 - S_1\cdot 1\cdot x = 1 + S_1x$.

By (10), the conditions $\delta^{(1)} = S_1 \neq 0$ and $2l^{(0)} = 2\cdot 0 = 0 \leq k - 1 = 1 - 1 = 0$ are satisfied. Then compute $\lambda^{(1)}(x) = \mu^{(0)}(x) = 1$, $l^{(1)} = k - l^{(0)} = 1 - 0 = 1$, and $\gamma^{(1)} = \delta^{(1)} = S_1$, respectively. Go to step 2.

Set $k = k + 1 = 1 + 1 = 2$. By (8), compute $\delta^{(2)} = \sum_{j=0}^{l^{(1)}=1} \mu_j^{(1)} S_{2-j} = \mu_0^{(1)} S_2 + \mu_1^{(1)} S_1 = 1\cdot S_2 + S_1S_1 = 0$.

By (9), compute $\mu^{(2)}(x) = \gamma^{(1)}\mu^{(1)}(x) - \delta^{(2)}\lambda^{(1)}(x)x = S_1(1 + S_1x) - 0\cdot 1\cdot x = S_1 + S_1^2x$.

By (10), the condition $\delta^{(2)} = 0$ is satisfied. Then compute $\lambda^{(2)}(x) = x\lambda^{(1)}(x) = x$, $l^{(2)} = l^{(1)} = 1$, and $\gamma^{(2)} = \gamma^{(1)} = S_1$, respectively. Go to step 2.

Set $k = k + 1 = 2 + 1 = 3$. By (8), compute $\delta^{(3)} = \sum_{j=0}^{l^{(2)}=1} \mu_j^{(2)} S_{3-j} = \mu_0^{(2)} S_3 + \mu_1^{(2)} S_2 = S_1S_3 + S_1^2S_2 = S_1S_3 + S_1^4$.

By (9), compute $\mu^{(3)}(x) = \gamma^{(2)}\mu^{(2)}(x) - \delta^{(3)}\lambda^{(2)}(x)\cdot x = S_1(S_1 + S_1^2x) - (S_1S_3 + S_1^4)\cdot x\cdot x = S_1^2 + S_1^3x + (S_1S_3 + S_1^4)x^2$.

By (10), the conditions $\delta^{(3)} \neq 0$ and is $2l^{(2)} = 2 \leq k - 1 = 3 - 1 = 2$. Compute $\lambda^{(3)}(x) = \mu^{(2)}(x) = S_1 + S_1^2x$, $l^{(3)} = k - l^{(2)} = 3 - 1 = 2$, and $\gamma^{(3)} = \delta^{(3)} = S_1S_3 + S_1^4$, respectively. Go to step 2.

Set $k = k + 1 = 3 + 1 = 4$. By (8), compute. $\delta^{(4)} = \sum_{j=0}^{l^{(3)}=2} \mu_j^{(3)} S_{4-j} = \mu_0^{(3)} S_4 + \mu_1^{(3)} S_3 + \mu_2^{(3)} S_2 = S_1^2S_4 + S_1^3S_3 + (S_1S_3 + S_1^4)S_2 = 0$.

By (9), compute $\mu^{(4)}(x) = \gamma^{(3)}\mu^{(3)}(x) - \delta^{(4)}\lambda^{(3)}(x)\cdot x = (S_1S_3 + S_1^4)(S_1^2 + S_1^3x + (S_1S_3 + S_1^4)x^2) - 0(S_1 + S_1^2x)x = (S_1^3S_3 + S_1^6) + (S_1^7 + S_1^4S_3)x + (S_1^2S_3^2 + S_1^8)x^2$.

By (10), the condition in is $\delta^{(4)} = 0$ is satisfied. Then compute $\lambda^{(4)}(x) = x\lambda^{(3)}(x) = x(S_1 + S_1^2x) = S_1x + S_1^2x^2$, $l^{(4)} = l^{(3)} = 2$, and $\gamma^{(4)} = \gamma^{(3)} = S_1S_3 + S_1^4$, respectively. Go to step 2.

Table 4. The Simplified Decoding Procedure for Example 2

k	$\mu^{(k)}(x)$	$\lambda^{(k)}(x)$	$l^{(k)}$	$\gamma^{(k)}$	$\delta^{(k)}$
0	1	1	0	1	-
1	$1 + S_1x$	1	1	S_1	S_1
2	$S_1 + S_1^2x$	x	1	S_1	0
3	$S_1^2 + S_1^3x + (S_1S_3 + S_1^4)x^2$	$S_1 + S_1^2x$	2	$S_1S_3 + S_1^4$	$S_1S_3 + S_1^4$
4	$(S_1^3S_3 + S_1^6) + (S_1^7 + S_1^4S_3)x + (S_1^2S_3^2 + S_1^8)x^2$	$S_1x + S_1^2x^2$	2	$S_1S_3 + S_1^4$	0
5	$(S_1^{10} + S_1^4S_3^2) + (S_1^{11} + S_1^5S_3^2)x + (S_1^6S_3^2 + S_1^9S_3)x^2 + (S_1^{13} + S_1^4S_3^3)x^3$	$(S_1^3S_3 + S_1^6) + (S_1^7 + S_1^4S_3)x + (S_1^2S_3^2 + S_1^8)x^2$	3	$S_1^{11} + S_1^2S_3^3$	$S_1^{11} + S_1^2S_3^3$
6	$(S_1^{21} + S_1^6S_3^5 + S_1^{12}S_3^3 + S_1^{15}S_3^2) + (S_1^{22} + S_1^{16}S_3^2 + S_1^{13}S_3^3 + S_1^7S_3^5)x + (S_1^{20}S_3 + S_1^{17}S_3^2 + S_1^{11}S_3^4 + S_1^8S_3^5)x^2 + (S_1^{24} + S_1^6S_3^6)x^3$	$(S_1^3S_3 + S_1^6)x + (S_1^7 + S_1^4S_3)x^2 + (S_1^2S_3^2 + S_1^8)x^3$	3	$S_1^{11} + S_1^2S_3^3$	0
7	Stop				

Set $k = k + 1 = 4 + 1 = 5$. By (8), compute $\delta^{(5)} = \sum_{j=0}^{l^{(4)}=2} \mu_j^{(4)} S_{5-j} = \mu_0^{(4)} S_5 + \mu_1^{(4)} S_4 + \mu_2^{(4)} S_3$ = $(S_1^3 S_3 + S_1^6)0 + (S_1^7 + S_1^4 S_3)S_4 + (S_1^2 S_3^2 + S_1^8)S_3 = S_1^{11} + S_1^2 S_3^3$.

By (9), compute $\mu^{(5)}(x) = \gamma^{(4)}\mu^{(4)}(x) - \delta^{(5)}\lambda^{(4)}(x)\cdot x = (S_1 S_3 + S_1^4)((S_1^3 S_3 + S_1^6) + (S_1^7 + S_1^4 S_3)x + (S_1^2 S_3^2 + S_1^8)x^2) - (S_1^{11} + S_1^2 S_3^3)(S_1 x + S_1^2 x^2)x = (S_1^{10} + S_1^4 S_3^2) + (S_1^{11} + S_1^5 S_3^2)x + (S_1^6 S_3^2 + S_1^9 S_3)x^2 + (S_1^{13} + S_1^4 S_3^3)x^3$.

By (10), the conditions $\delta^{(4)} \neq 0$ and $2l^{(k-1)} = 2l^{(4)} = 4 \leq k - 1 = 5 - 1 = 4$ are satisfied. Then compute $\lambda^{(5)}(x) = \mu^{(4)}(x) = (S_1^3 S_3 + S_1^6) + (S_1^7 + S_1^4 S_3)x + (S_1^2 S_3^2 + S_1^8)x^2$, $l^{(5)} = k - l^{(4)} = 5 - 2 = 3$, and $\gamma^{(5)} = \delta^{(5)} = S_1^{11} + S_1^2 S_3^3$, respectively. Go to step 2.

Set $k = k + 1 = 5 + 1 = 6$. By (8), compute $\delta^{(6)} = \sum_{j=0}^{l^{(5)}=3} \mu_j^{(5)} S_{6-j} = \mu_0^{(5)} S_6 + \mu_1^{(5)} S_5 + \mu_2^{(5)} S_4 + \mu_3^{(5)} S_3$ = $(S_1^{10} + S_1^4 S_3^2)S_6 + (S_1^{11} + S_1^5 S_3^2)S_5 + (S_1^6 S_3^2 + S_1^9 S_3)S_4 + (S_1^{13} + S_1^4 S_3^3)S_3 = 0$.

By (9), compute the error-locator polynomial of degree 3, $\mu^{(6)}(x) = \gamma^{(5)}\mu^{(5)}(x) - \delta^{(6)}\lambda^{(5)}(x)x = (S_1^{11} + S_1^2 S_3^3)(S_1^{10} + S_1^4 S_3^2) + (S_1^{11} + S_1^5 S_3^2)x + (S_1^6 S_3^2 + S_1^9 S_3)x^2 + (S_1^{13} + S_1^4 S_3^3)x^3) - 0((S_1^3 S_3 + S_1^6) + (S_1^7 + S_1^4 S_3)x + (S_1^2 S_3^2 + S_1^8)x^2)x = (S_1^{21} + S_1^6 S_3^5 + S_1^{12} S_3^3 + S_1^{15} S_3^2) + (S_1^{22} + S_1^{16} S_3^2 + S_1^{13} S_3^3 + S_1^7 S_3^5)x + (S_1^{20} S_3 + S_1^{17} S_3^2 + S_1^{11} S_3^4 + S_1^8 S_3^5)x^2 + (S_1^{24} + S_1^6 S_3^6)x^3$.

By (10), the condition $\delta^{(6)} = 0$ is satisfied. Then compute $\lambda^{(6)}(x) = x\lambda^{(5)}(x) = x((S_1^3 S_3 + S_1^6) + (S_1^7 + S_1^4 S_3)x + (S_1^2 S_3^2 + S_1^8)x^2) = (S_1^3 S_3 + S_1^6)x + (S_1^7 + S_1^4 S_3)x^2 + (S_1^2 S_3^2 + S_1^8)x^3$, $l^{(6)} = l^{(5)} = 3$, and $\gamma^{(6)} = \gamma^{(5)} = S_1^{11} + S_1^2 S_3^3$, respectively. Go to step 2.

Set $k = k + 1 = 6 + 1 = 7$. Since $k = 7 > 2t = 6$, go to stop.

The above decoding procedure is simplified in Table 4. When $k = 6$, one obtains the error-locator polynomial $\mu^{(6)}(x) = L(x) = (S_1^{21} + S_1^6 S_3^5 + S_1^{12} S_3^3 + S_1^{15} S_3^2) + (S_1^{22} + S_1^{16} S_3^2 + S_1^{13} S_3^3 + S_1^7 S_3^5)x + (S_1^{20} S_3 + S_1^{17} S_3^2 + S_1^{11} S_3^4 + S_1^8 S_3^5)x^2 + (S_1^{24} + S_1^6 S_3^6)x^3$, which means that $\mu^{(6)}(x)$ has three roots. By applying Chien search algorithm, the roots of $L(x)$ are exactly the inverse of the three error locators {0, 1, 19}. For example, the third error locator is α^{19}, and the reciprocal of α^{19} is α^{12}. Substituting α^{12} into $L(x)$, then the error-locator polynomial $L(\alpha^{12}) = ((\alpha^5)^{21} + (\alpha^5)^6(\alpha^{24})^5 + (\alpha^5)^{12}(\alpha^{24})^3 + (\alpha^5)^{15}(\alpha^{24})^2) + ((\alpha^5)^{22} + (\alpha^5)^{16}(\alpha^{24})^2 + (\alpha^5)^{13}(\alpha^{24})^3 + (\alpha^5)^7(\alpha^{24})^5)\alpha^{12} + ((\alpha^5)^{20}(\alpha^{24}) + (\alpha^5)^{17}(\alpha^{24})^2 + (\alpha^5)^{11}(\alpha^{24})^4 + (\alpha^5)^8(\alpha^{24})^5)(\alpha^{12})^2 + ((\alpha^5)^{24} + (\alpha^5)^6(\alpha^{24})^6)(\alpha^{12})^3 = \alpha^{12} + \alpha^{26} + \alpha^8 + \alpha^{30} + (\alpha^{17} + \alpha^4 + \alpha^{13} + 1)\alpha^{12} + (1 + \alpha^9 + \alpha^{27} + \alpha^5)\alpha^{24} + (\alpha^{27} + \alpha^{19})\alpha^5 = \alpha^{12} + \alpha^{26} + \alpha^8 + \alpha^{30} + \alpha^{29} + \alpha^{16} + \alpha^{25} + \alpha^{12} + \alpha^{24} + \alpha^2 + \alpha^{20} + \alpha^{29} + \alpha + \alpha^{24} = 0$. Similarly, the first and the second error locators are $\alpha^0 = 1$ and α, then we obtain $L(1) = 0$ and $L(\alpha^{30}) = 0$, respectively. A C++ program shows that the total 155 weight-3 error patterns with $S_5 = 0$ can be corrected.

For the primary known syndrome S_7, there are also 155 weight-3 error patterns are equal to zero. However, the IFBM algorithm does not use S_7 to decode the weight-3 error patterns.

4. Conclusions

For the QR codes with irreducible generator polynomial, the primary known syndrome S_1 cannot be equal to zero while the IFBM algorithm is used to determine the error-locator polynomial. In this paper, two examples with detailed step-by-step analysis show that the IFBM algorithm can obtain an valid error-locator polynomial for the (31, 16, 7) QR code with reducible generator polynomial in GF(2^5). However, the determination of the error-locator polynomial by using the IFBM is time-consuming. An efficient condition may be added in the IFBM to reduce the decoding time in the future.

REFERENCES

[1] E. Prange, "Cyclic error-correcting codes in two symbols," AFCRC-TN-57-103, Air Force Cambridge Research Center, Cambridge, Mass. 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, 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, 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, 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, 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, 2001.

[8] 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, 2003.

[9] T. K. Truong, Y. Chang, Y. H. Chen and C. D. Lee, "Algebraic Decoding of (103, 52, 19) and (113, 57, 15) Quadratic Residue Code," IEEE Trans. on Comm., vol. 53, no. 5, pp. 749–754, 2005.

[10] 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," J. Inf. Sci. Eng., vol. 23, no. 1, pp. 127–145, 2007.

[11] 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, 2008.

[12] T. C. Lin, S. I. Chu, H. C. Chang, and H. P. Lee, "Decoding the (31, 16, 7) Quadratic Residue Code in GF(2^5)," The 4th

International Conference on Computer Science and Education (ICCSE 2009), Nanning, China, 2009.

[13] 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, 2009.

[14] T. C. Lin、P. Y. Shih、W. K. Su、T. K. Truong, "Algebraic decoding of the (31, 16, 7) quadratic residue code by using Berlekamp-Massey algorithm," 2010 International Conference on Communications and Mobile Computing (CMC 2010), Shenzhen, China, pp. 275–277, 2010.

[15] 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, 2010.

[16] H. P. Lee, H. C. Chang, and T. K. Truong, "Algebraic decoding of the (73, 37, 13) quadratic residue code," IET Communications, vol. 6, no. 10, pp. 1326–1333, 2012.

[17] 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,. 1994.

[18] 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, 1991.

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

[20] H. P. Lee, "A viewpoint on the decoding of the quadratic residue code of Length 89," International Journal of Networks and Communications, vol. 2, no. 1, pp. 11–16, 2012.