JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 23, 127-145 (2007)

Algebraic Decoding of Quadratic Residue Codes Using Berlekamp-Massey Algorithm*

Y. H. CHEN, T. K. TRUONG, Y. CHANG, C. D. LEE AND S. H. CHEN+
School of Electrical and Information Engineering
I-Shou University
Kaohsiung, 840 Taiwan
+*Department of Computer Science and Information Engineering*
Shu-Te University
Kaohsiung, 824 Taiwan

In this paper, an algebraic decoding method is proposed for the quadratic residue codes that utilize the Berlekamp-Massey algorithm. By a modification of the technique developed by He *et al*., one can express the unknown syndromes as functions of the known syndromes. The unknown syndromes are determined by an efficient algorithm also developed in this paper. With the appearance of unknown syndromes, one obtains the consecutive syndromes that are needed for the application of the Berlekamp-Massey algorithm. The decoding scheme, developed here, is easier to implement than the previous decoding algorithm developed for the Golay code and the (47, 24, 11) QR code. Moreover, it can be extended to decode all codes of the family of binary quadratic residue codes with irreducible generating polynomials.

Keywords: quadratic residue codes, unknown syndromes, known syndromes, Berlekamp-Massey algorithm, error-locator polynomial

1. INTRODUCTION

The quadratic residue (QR) codes were introduced by Prange in his 1958 paper [1]. They are cyclic codes that of high rates, approximately one-half. The known QR codes have reasonably large minimum distances, so that most of them are the best known codes. Their performance as part of a concatenated code, for example, a Reed-Solomon (RS) code and a QR code compares favorably with the concatenation of the same RS code and the corresponding convolutional code, *e.g.* see [2]. However, QR codes have two nice properties: Firstly, QR codes are block codes, and secondly, QR codes are algebraically decodable in a polynomial number of operations. With these merits, QR codes are very good codes to use for concatenated codes. Thus there is a need for efficient algorithms to decode QR codes. Recently, much work on the algebraic decoding of QR codes has increased the number of applications [3-8]. Except for the (23, 12, 7) QR code [7], namely, the Golay code, the techniques most used to decode the QR codes are the Newton identities with either Sylvester resultants or Gröbner bases. The difficulty of these approaches is that one has to solve equations in many variables, obtained from the Newton identities [8]. Also, different QR codes have different sets of conditions for determining the posi-

Received November 24, 2004; revised March 21, 2005; accepted March 31, 2005.
Communicated by Liang-Gee Chen.
* This work were supported by the National Science Council of Taiwan, R.O.C., under grants NSC 93-2213-E-214-001 and NSC 93-2215-M-214-003.

tions of errors in the decoding algorithms. In this paper, the well-known Berlekamp-Massey (BM) algorithm [9, 10] is used to decode the QR codes in a different approach. The idea of finding the unknown syndromes [3, 11] to complete the syndromes list makes it possible to apply the very efficient BM algorithm to the decoding of the QR codes. The unknown syndromes are determined in this paper by the efficient algorithm developed in section 2 to calculate the unknown syndromes.

Finally, this decoding method is verified by a software simulation that uses the C++ language. This simulation demonstrates the systematic decoding of a QR code by a use of the inverse-free BM algorithm.

This paper is organized as follows: Section 2 gives the basic terminology of the QR codes and defines the unknown syndromes. Also, an efficient algorithm for calculating unknown syndromes is introduced in this section. Section 3 is the main body of this paper; it demonstrates the unknown syndrome technique, developed in section 2 as well as the inverse-free BM algorithm [12] to decode the (47, 24, 11) QR code. Finally, a completely work-outed example, using the (23, 12, 7) QR code, is demonstrated in detail. The final section gives some concluding remarks about the decoding scheme developed in this paper.

2. PRELIMINARY AND TERMINOLOGY

2.1 Basic Terminology

In this paper, QR codes are introduced by describing the properties of the (47, 24, 11) QR code and subsequently those of the Golay code. As usual, let $E = GF(2^{23})$ be the defining field of the (47, 24, 11) QR code. To introduce the binary (47, 24, 11) QR code, one first computes the set of quadratic residues, modulo 47, Q_{47} as follows:

$$\begin{aligned} Q_{47} &= \{i \mid i \equiv j^2 \bmod 47 \text{ for } 1 \le j \le 46\} \\ &= \{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}. \end{aligned} \quad (1)$$

If α is a primitive element of E, then $\beta = \alpha^{178481}$ is a primitive 47th root of unity in E. The QR code of length $n = 47$ is a cyclic code with the generator polynomial $g(x)$ defined by

$$\begin{aligned} g(x) = \prod_{i \in Q_n} (x - \beta^i) &= x^{23} + x^{19} + x^{18} + x^{14} + x^{13} + x^{12} + x^{10} + x^9 + x^7 \\ &+ x^6 + x^5 + x^3 + x^2 + x + 1. \end{aligned} \quad (2)$$

A binary vector $\boldsymbol{c} = (c_0, c_1, \ldots, c_{46})$ is a codeword if and only if its associated polynomial $c(x) = c_0 + c_1x + \ldots + c_{46}x^{46}$ is a multiple of $g(x)$. If $\boldsymbol{r} = (r_0, r_1, \ldots, r_{46})$ is a received vector, then its associated polynomial $r(x) = r_0 + r_1x + \ldots + r_{46}x^{46}$ can be expressed as a sum of the transmitted code polynomial $c(x)$ and the error polynomial $e(x) = e_0 + e_1x + \ldots + e_{46}x^{46}$. The set of known *syndromes* is obtained by evaluating $r(x)$ at the roots of $g(x)$, namely

$$S_i = r(\beta^i) = c(\beta^i) + e(\beta^i) = e(\beta^i) = e_0 + e_1\beta + \ldots + e_{46}\beta^{46} \tag{3}$$

for $i \in Q_{47}$. If v errors occur in the received vector, then the error polynomial has v nonzero terms, namely, $e(x) = x^{r_1} + x^{r_2} + x^{r_3} + \ldots + x^{r_v}$, where $0 \le r_1 < r_2 < \ldots < r_v \le 46$. For $i \in Q_{47}$, the ith syndrome S_i is given by

$$S_i = (\beta^{r_1})^i + (\beta^{r_2})^i + \ldots + (\beta^{r_v})^i = Z_1^i + Z_2^i + \ldots + Z_v^i, \tag{4}$$

where $Z_j = \beta^{r_j}$ for $1 \le j \le v$, are called the error locators.

For the (47, 24, 11) QR code, one has the following equalities among the known syndromes as $S_2 = S_1^2$, $S_4 = S_1^{2^2}$, $S_8 = S_1^{2^3}$, $S_{16} = S_1^{2^4}$, $S_{32} = S_1^{2^5}$, $S_{17} = S_1^{2^6}$, $S_{34} = S_1^{2^7}$, $S_{21} = S_1^{2^8}$, $S_{42} = S_1^{2^9}$, $S_{37} = S_1^{2^{10}}$, $S_{27} = S_1^{2^{11}}$, $S_7 = S_1^{2^{12}}$, $S_{14} = S_1^{2^{13}}$, $S_{28} = S_1^{2^{14}}$, $S_9 = S_1^{2^{15}}$, $S_{18} = S_1^{2^{16}}$, $S_{36} = S_1^{2^{17}}$, $S_{25} = S_1^{2^{18}}$, $S_3 = S_1^{2^{19}}$, $S_6 = S_1^{2^{20}}$, $S_{12} = S_1^{2^{21}}$, and $S_{24} = S_1^{2^{22}}$.

To determine the error locators Z_i's, define the error-locator polynomial $\sigma(z)$ as follows:

$$\sigma(z) = \prod_{j=1}^{v}(1 + Z_j z) = 1 + \sum_{j=1}^{v}\sigma_j z^j, \tag{5}$$

where

$$\sigma_1 = Z_1 + Z_2 + \ldots + Z_v,\ \sigma_2 = Z_1Z_2 + Z_1Z_3 + \ldots + Z_{v-1}Z_v = \sum_{1 \le i < j \le v} Z_iZ_j,\ \ldots, \text{ and}$$
$$\sigma_v = Z_1Z_2 \ldots Z_v.$$

The error-locator polynomial $\sigma(z)$ can be obtained by applying the BM algorithm. It is well known that the BM algorithm is an efficient method for determining the error-locator polynomial when used to decode both the RS codes and BCH codes. In this paper, One uses it to decode both the (47, 24, 11) QR code and the Golay code. It can also be used to decode any binary QR codes with irreducible generating polynomial, for example [13]. In order to employ the BM algorithm to decode a code up to 5 errors, one needs in sequence the ten syndromes, S_1, S_2, …, S_9, S_{10}. For the (47, 24, 11) code, the minimal distance is 11. It can correct up to 5 errors; however, the only syndromes that can be determined directly from $r(x)$ are S_1, S_2, S_3, S_4, S_6, S_7, S_8 and S_9. The two syndromes $S_5 = Z_1^5 + Z_2^5 + \ldots + Z_v^5$ and $S_{10} = S_5^2$ are absent. They cannot be obtained by evaluating $r(x)$ at the roots of $g(x)$. The procedure given in [3, 11] 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. 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. Next, define a matrix $X(I)$ of size $(v + 1) \times v$ as shown below:

$$X(I) = \begin{bmatrix} Z_1^{i_1} & Z_2^{i_1} & \cdots & Z_v^{i_1} \\ Z_1^{i_2} & Z_2^{i_2} & \cdots & Z_v^{i_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{i_v} & Z_2^{i_v} & \cdots & Z_v^{i_v} \\ Z_1^{i_{v+1}} & Z_2^{i_{v+1}} & \cdots & Z_v^{i_{v+1}} \end{bmatrix}. \tag{6}$$

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:

$$S(I, J) = X(I)X(J)^T, \tag{7}$$

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

$$S(I, J) = \begin{bmatrix} S_{i_1+j_1} & S_{i_1+j_2} & \cdots & S_{i_1+j_{v+1}} \\ S_{i_2+j_1} & S_{i_2+j_2} & \cdots & S_{i_2+j_{v+1}} \\ \vdots & \vdots & \ddots & \vdots \\ S_{i_v+j_1} & S_{i_v+j_2} & \cdots & S_{i_v+j_{v+1}} \\ S_{i_{v+1}+j_1} & S_{i_{v+1}+j_2} & \cdots & S_{i_{v+1}+j_{v+1}} \end{bmatrix}, \tag{8a}$$

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.*,

$$\det(S(I, J)) = 0. \tag{8b}$$

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 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

$$S_r = \frac{\det(\Delta_0)}{\det(\Delta)}, \tag{9}$$

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 1 and 2 are given in the Appendix. Theorem 2 is used to determine the primary unknown syndrome S_5 of (47, 24, 11) QR code by searching for the two subsets I and J of $\{0, 1, \ldots, 46\}$ such that matrix $S(I, J)$ contains the unknown syndrome S_5 as its entry only once. To do this, an exhaustive search needs at most $(C_{v+1}^{47})^2$ choices, where $C_{v+1}^{47} = (47!)/((47 - (v + 1))!(v + 1)!)$ is the binomial coefficient for the number of combinations taking $v + 1$ from a set of 47 elements. The algorithm developed next reduces the number of tries so that only C_{v+1}^{25} choices are needed for an exhaustive search to find S_5.

For the (47, 24, 11) QR code, the primary unknown syndrome is S_5. Let $Q = Q_{47} \cup \{0, 5\}$. Before stating the algorithm, one needs some more notations. For $i \in Q$, define the difference of i from Q to be:

$$Q - i = \{(q - i) \bmod 47 \mid q \in Q\}.$$

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 $I \oplus J = \{(i + j) \bmod 47 \mid i \in I, j \in J\}^*$, where one uses a star-sign "*" to indicate that the set is a multi-set.

For example, let $v = 2$ and $i = 1$. Then the difference of 1 from Q is

$$\begin{aligned} Q - 1 &= \{(q - 1) \bmod 47 \mid q \in Q\} = \{0 - 1, 1 - 1, \ldots, 42 - 1\} \\ &= \{46, 0, 1, 2, 3, 5, 6, 7, 8, 11, 13, 15, 16, 17, 20, 23, 24, 26, 27, 31, 33, 35, 36, 41\}. \end{aligned}$$

Next, let $v = 2$, $I = \{1, 2, 3\}$ and $J = \{0, 1, 2\}$. Then

$$\begin{aligned} I \oplus J &= \{1 + 0, 1 + 1, 1 + 2, 2 + 0, 2 + 1, 2 + 2, 3 + 0, 3 + 1, 3 + 2\}^* \\ &= \{1, 2, 3, 2, 3, 4, 3, 4, 5\}^* = \{1, 2, 2, 3, 3, 3, 4, 4, 5\}^*. \end{aligned}$$

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 1

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

Step 2: Check the number of elements in the intersection $(Q - i_1) \cap (Q - i_2) \cap \ldots \cap (Q - i_{v+1})$.
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. (9), 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. Using the efficiency of

this algorithm, the number of choices can be substantially reduced. Table 1 shows that the numbers of choices of both the fast method and the direct method and also in the ratio saved that may be saved by running the fast method. The comparisons for various cases for different numbers of errors are given in Table 1. One observes from Table 1 that the fast method requires only a small fraction of the number of choices that are required in a direct method.

Table 1. The number of choices for various cases of different number of errors.

V	Direct method $(C_{v+1}^{47})^2$	Fast method C_{v+1}^{25}	Ratio saved $(C_{v+1}^{25}/(C_{v+1}^{47})^2)\times 100\,\%$
2	2.6×10^8	2.3×10^3	$8.8 \times 10^{-4}\%$
3	3.2×10^{10}	1.3×10^4	$4.0 \times 10^{-5}\%$
4	2.4×10^{12}	5.3×10^4	$2.3 \times 10^{-6}\%$
5	1.2×10^{14}	1.8×10^5	$1.5 \times 10^{-7}\%$

3. ALGEBRAIC DECODER FOR (47, 24, 11) QR CODE USING THE BM ALGORITHM

This section is the main part of the paper. It illustrates the ideas needed to decode the (47, 24, 11) QR code. There are two subsections: The first subsection describes how to determine the primary unknown syndrome, S_5, 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 ten known syndromes, including the two calculated unknown syndromes, for the (47, 24, 11) 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 $r \in \{5, 10\}$, $S_r^{(v)}$ denotes the unknown syndrome S_r for the v-errors case.

3.1 Determination of the Unknown Syndrome S_5

The six cases from case 0 to case 5 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_5. Moreover, the attachment of a super-index to "S_5" to obtain the notation "$S_5^{(v)}$" indicates that it is valid for the v-error case only.

Case 0: (0 error)

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

Case 1: (1 error)

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

Case 2: (2 errors)

Assume the number of errors is two, *i.e.* $v = 2$. Let $I_2 = \{0, 3, 7\}$ and $J_2 = \{0, 1, 2\}$. Then one obtains the following matrix from Theorem 1:

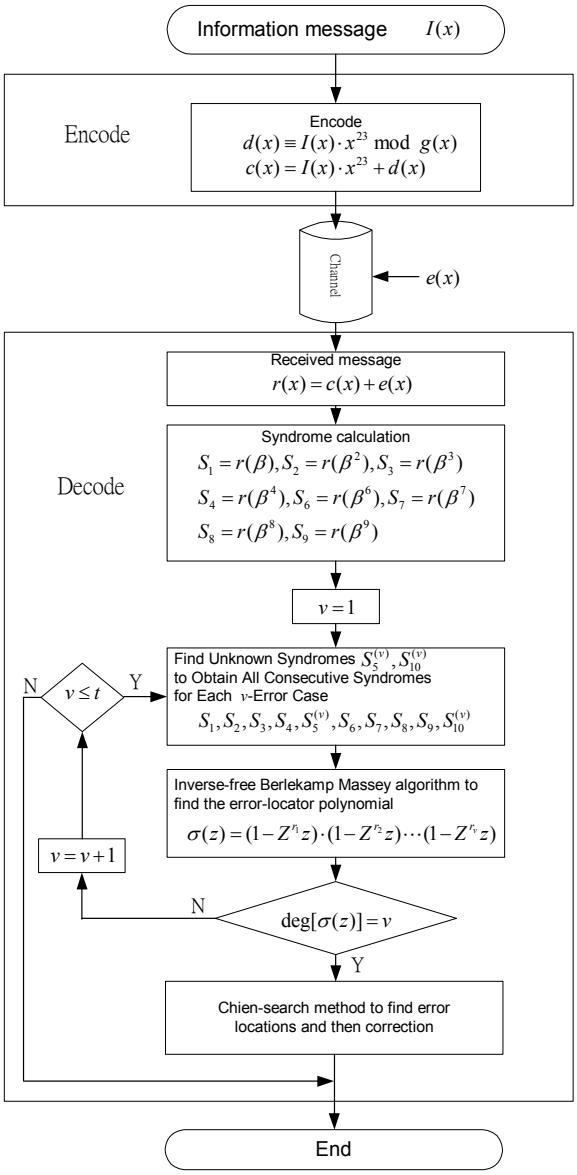


Fig. 1. Flowchart of the (47, 24, 11) QR code encoder and decoder.

$$S(I_2, J_2) = \begin{bmatrix} S_0 & S_3 & S_7 \\ S_1 & S_4 & S_8 \\ S_2 & S_5^{(2)} & S_9 \end{bmatrix}, \tag{10}$$

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

$$S_5^{(2)} = \frac{\det(\Delta_0)}{\det(\Delta)} = (S_2S_3S_8 + S_2S_4S_7 + S_1S_3S_9) / S_1S_7. \tag{11}$$

Case 3: (3 errors)

Let $I_3 = \{0, 1, 2, 5\}$ and $J_3 = \{0, 1, 7, 16\}$. Then, by Theorem 1, one obtains

$$S(I_3, J_3) = \begin{bmatrix} S_0 & S_1 & S_2 & S_5^{(3)} \\ S_1 & S_2 & S_3 & S_6 \\ S_7 & S_8 & S_9 & S_{12} \\ S_{16} & S_{17} & S_{18} & S_{21} \end{bmatrix}, \tag{12}$$

where $S_0 = 1$. Thus one can solve for the unknown syndrome $S_5^{(3)}$ for 3-error case as follows:

$$S_5^{(3)} = \frac{\det(\Delta_0)}{\det(\Delta)}, \tag{13}$$

where

$$\Delta = \begin{bmatrix} S_1 & S_2 & S_3 \\ S_7 & S_8 & S_9 \\ S_{16} & S_{17} & S_{18} \end{bmatrix} \text{ and } \Delta_0 = \begin{bmatrix} S_0 & S_1 & S_2 & 0 \\ S_1 & S_2 & S_3 & S_6 \\ S_7 & S_8 & S_9 & S_{12} \\ S_{16} & S_{17} & S_{18} & S_{21} \end{bmatrix}. \tag{14}$$

Case 4: (4 errors)

Let $I_4 = \{0, 1, 2, 18, 21\}$ and $J_4 = \{0, 3, 6, 7, 16\}$. Then, again by Theorem 1, one obtains

$$S(I_4, J_4) = \begin{bmatrix} S_0 & S_1 & S_2 & S_{18} & S_{21} \\ S_3 & S_4 & S_5^{(4)} & S_{21} & S_{24} \\ S_6 & S_7 & S_8 & S_{24} & S_{27} \\ S_7 & S_8 & S_9 & S_{25} & S_{28} \\ S_{16} & S_{17} & S_{18} & S_{34} & S_{37} \end{bmatrix}, \tag{15}$$

where $S_0 = 0$. By Theorem 2, the unknown syndrome $S_5^{(4)}$ for 4-error case can be found as follows:

$$S_5^{(4)} = \frac{\det(\Delta_0)}{\det(\Delta)}, \tag{16}$$

where

$$\Delta = \begin{bmatrix} S_0 & S_1 & S_{18} & S_{21} \\ S_6 & S_7 & S_{24} & S_{27} \\ S_7 & S_8 & S_{25} & S_{28} \\ S_{16} & S_{17} & S_{34} & S_{37} \end{bmatrix} \text{ and } \Delta_0 = \begin{bmatrix} S_0 & S_1 & S_2 & S_{18} & S_{21} \\ S_3 & S_4 & 0 & S_{21} & S_{24} \\ S_6 & S_7 & S_8 & S_{24} & S_{27} \\ S_7 & S_8 & S_9 & S_{25} & S_{28} \\ S_{16} & S_{17} & S_{18} & S_{34} & S_{37} \end{bmatrix}. \tag{17}$$

In the 5-error case there does not exist a pair of subsets $I, J \subset \{0, 1, \ldots, 46\}$ such that S_5 appears exactly once in the matrix $S(I, J)$. This is proved by an exhaustive computer search using the efficient algorithm given in the previous section.

Case 5: (5 errors)

When the number of errors is five, the case is more complicated. First, let $I_5^1 = \{0, 1, 4, 8, 12, 32\}$ and $J_5^1 = \{0, 2, 4, 16, 20, 24\}$. Then one obtains the matrix,

$$S(I_5^1, J_5^1) = \begin{bmatrix} S_0 & S_1 & S_4 & S_8 & S_{12} & S_{32} \\ S_2 & S_3 & S_6 & \boxed{S_{10}} & S_{14} & S_{34} \\ S_4 & \boxed{S_5} & S_8 & S_{12} & S_{16} & S_{36} \\ S_{16} & S_{17} & \boxed{S_{20}} & S_{24} & S_{28} & S_1 \\ \boxed{S_{20}} & S_{21} & S_{24} & S_{28} & S_{32} & \boxed{S_5} \\ S_{24} & S_{25} & S_{28} & S_{32} & S_{36} & S_9 \end{bmatrix}. \tag{18}$$

By Eq. (1), the syndromes in the boxes are unknown and function of S_5. They are S_5, $S_{10} = S_5^2$ and $S_{20} = S_5^4$ with the syndromes $S_0 = 1$. A substitution of these quantities $S(I_5^1, J_5^1)$ in Eq. (18) yields an 11th degree polynomial in S_5, say $f(S_5)$, as follows:

$$f(S_5) = \sum_{i=0}^{11} a_i (S_5)^i, \tag{19}$$

where the leading coefficient of $f(S_5)$ is $a_{11} = S_9 S_{12} + S_{32} S_{36}$.

Next, another 11the degree polynomial can be found by choosing another different pair (I_5^2, J_5^2) of subsets of $\{0, 1, \ldots, 46\}$. Let $I_5^2 = \{0, 1, 2, 4, 8, 12\}$ and $J_5^2 = \{0, 2, 4, 6, 8, 16\}$. Then, one has another matrix,

$$S(I_5^2, J_5^2) = \begin{bmatrix} S_0 & S_1 & S_2 & S_4 & S_8 & S_{12} \\ S_2 & S_3 & S_4 & S_6 & \boxed{S_{10}} & S_{14} \\ S_4 & \boxed{S_5} & S_6 & S_8 & S_{12} & S_{16} \\ S_6 & S_7 & S_8 & \boxed{S_{10}} & S_{14} & S_{18} \\ S_8 & S_9 & \boxed{S_{10}} & S_{12} & S_{16} & \boxed{S_{20}} \\ S_{16} & S_{17} & S_{18} & \boxed{S_{20}} & S_{24} & S_{28} \end{bmatrix}. \tag{20}$$

Expanding the determinant $\det(S(I_5^2, J_5^2))$, one obtains an 11th degree polynomial $g(S_5) = \det(S(I_5^2, J_5^2))$ different from $f(S_5)$ as follows:

$$g(S_5) = \sum_{i=0}^{11} b_i (S_5)^i, \tag{21}$$

where the leading coefficient of $g(S_5)$ is $b_{11} = S_2 S_6 + S_8$.

Let $F(S_5)$ be the greatest common divisor of polynomials $f(S_5)$ and $g(S_5)$, *i.e.* $F(S_5) = GCD(f(S_5), g(S_5))$. Since S_5 is a zero of both $f(S_5)$ and $g(S_5)$, S_5 is also a zero of $F(S_5) = GCD(f(S_5), g(S_5))$. Euclid's algorithm is used to run through all error patterns of weight 5, and a full computer search a show that, in each case, $F(S_5)$ is always a polynomial of degree 1. Thus, the needed unknown syndrome S_5 for 5-error case, *i.e.* $S_5^{(5)}$, can be determined uniquely.

3.2 The Inverse-Free Berlekamp-Massey Algorithm

To decode the (47, 24, 11) 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 $\gamma^{(0)} = 0$.
Step 2: Compute

$$\Delta^{(k)} = \sum_{j=0}^{\ell^{(k-1)}} c_j^{(k-1)} s_{k-j}, \tag{22}$$

where the coefficients $c^{(k-1)}$ are the coefficients of polynomial $C^{(k-1)}(x)$ at the $(k-1)$th stage.
Step 3: Compute

$$C^{(k)}(x) = \gamma^{(k-1)} \cdot C^{(k-1)}(x) - \Delta^{(k)} \cdot A^{(k-1)}(x) \cdot x. \tag{23}$$

Step 4:

$$A^{(k)}(x) = \begin{cases} x \cdot A^{(k-1)}(x) & \text{if } \Delta^{(k)} = 0 \text{ or } 2\ell^{(k-1)} > k-1 \\ C^{(k-1)}(x) & \text{if } \Delta^{(k)} \neq 0 \text{ and } 2\ell^{(k-1)} \leq k-1 \end{cases}, \tag{24}$$

$$\ell^{(k)} = \begin{cases} \ell^{(k-1)} & \text{if } \Delta^{(k)} = 0 \text{ or if } 2\ell^{(k-1)} > k-1 \\ k - \ell^{(k-1)} & \text{if } \Delta^{(k)} \neq 0 \text{ and if } 2\ell^{(k-1)} \leq k-1 \end{cases}, \tag{25}$$

$$\gamma^{(k)} = \begin{cases} \gamma^{(k-1)} & \text{if } \Delta^{(k)} = 0 \text{ or if } 2\ell^{(k-1)} > k-1 \\ \Delta^{(k)} & \text{if } \Delta^{(k)} \neq 0 \text{ and if } 2\ell^{(k-1)} \leq k-1 \end{cases}. \tag{26}$$

Step 5: Set $k = k + 1$ if $k \leq 2t$, then 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. (23).

To illustrate the above decoder for correcting errors, the algorithm is adopted to the (23, 12, 7) QR triple-errors correcting code over $GF(2^{11})$ generated by an irreducible primitive polynomial $p(x) = x^{11} + x^2 + 1$ over $GF(2)$. The details of this simple example of a QR code are given here instead of the (47, 24, 11) QR code. The set $Q_{23} = \{1, 2, 3, 4,$

6, 8, 9, 12, 13, 16, 18} constitute the quadratic residues, modulo 23. Also $\beta = \alpha^{89}$ is a primitive 23rd root of unity in $GF(2^{11})$, where α is a primitive element of $GF(2^{11})$ satisfies the equation, $\alpha^{11} + \alpha^2 + 1 = 0$. This code can correct 3 errors and the single unknown syndrome is S_5.

For the cases of errors, the unknown syndromes, the $S_5^{(v)}$'s, are determined as follows:

For $v = 1$, let $I_1 = \{1, 5\}$ and $J_1 = \{0, 3\}$. The matrix $S(I_1, J_1)$ of size 2×2 is

$$S(I_1, J_1) = \begin{bmatrix} S_1 & S_5^{(1)} \\ S_4 & S_8 \end{bmatrix}, \tag{27}$$

where $S_4 = S_1^4$ and $S_8 = S_1^8$.

For $v = 2$, let $I_2 = \{1, 2, 5\}$ and $J_2 = \{0, 7, 11\}$. The matrix $S(I_2, J_2)$ of size 3×3 is

$$S(I_2, J_2) = \begin{bmatrix} S_1 & S_2 & S_5^{(2)} \\ S_8 & S_9 & S_{12} \\ S_{12} & S_{13} & S_{16} \end{bmatrix}, \tag{28}$$

where $S_2 = S_1^2, S_9 = S_1^{32}, S_{12} = S_1^{1024}, S_{13} = S_1^{128}$, and $S_{16} = S_1^{16}$.

For $v = 3$, let $I_3 = \{0, 1, 4, 16\}$ and $J_3 = \{0, 2, 8, 12\}$. The matrix $S(I_3, J_3)$ of size 4×4 is given as follows:

$$S(I_3, J_3) = \begin{bmatrix} S_0 & S_1 & S_4 & S_{16} \\ S_2 & S_3 & S_6 & S_{18} \\ S_8 & S_9 & S_{12} & S_1 \\ S_{12} & S_{13} & S_{16} & S_5^{(3)} \end{bmatrix}, \tag{29}$$

where $S_0 = 1, S_3 = S_1^{256}, S_6 = S_1^{512}$, and $S_{18} = S_1^{64}$.

The generator polynomial of the (23, 12, 7) QR code is given by

$$g(x) = \prod_{i \in Q_{23}} (x - \beta^i) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1.$$

Assume the message vector is given as $\boldsymbol{I}$ = (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1). Multiplying its associated polynomial $I(x) = x^{10} + x^9 + x^5 + 1$ by $g(x)$, one obtains the code polynomial $c(x) = I(x) \cdot x^{11} + d(x) = x^{21} + x^{20} + x^{16} + x^{11} + x^9 + x^5 + x^2$ where $d(x)$ is the reminder of $I(x) \cdot x^{11}$ divided by $g(x)$. Let c be the code vector of this polynomial $\boldsymbol{c}$ = (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 1, 0, 0).

Three cases, cases 1 to 3, are discussed below. The number of the case indicates the number of errors that occur in the received code vector.

Case 1: For the case of one error case, assume the error vector is $\boldsymbol{e}$ = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0). Then the received vector is $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ = (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0) and its associated polynomial is $r(x) = x^{21} +$

$x^{20} + x^{16} + x^{11} + x^9 + x^5 + x^2 + x$. For $i = 1, 2, 3, 4$ and 6, the syndromes are

$$S_i = r(\beta^i) = (\beta^i)^{21} + (\beta^i)^{20} + (\beta^i)^{16} + (\beta^i)^{11} + (\beta^i)^9 + (\beta^i)^5 + (\beta^i)^2 + \beta^i.$$

That is, $S_1 = \alpha^{89}$, $S_2 = \alpha^{178}$, $S_3 = \alpha^{267}$, $S_4 = \alpha^{356}$, and $S_6 = \alpha^{534}$.

By a use of Eqs. (27) and (9), the single unknown syndrome for 1-error case is found to be $S_5^{(1)} = \alpha^{445}$. Using the inverse-free BM algorithm, the computation terminates at step $k = 6$, and one obtains $C^{(6)}(x) = \alpha^{534}x + \alpha^{445}$ from the consecutive known syndromes $S_1 = \alpha^{89}$, $S_2 = \alpha^{178}$, $S_3 = \alpha^{267}$, $S_4 = \alpha^{356}$, $S_5^{(1)} = \alpha^{445}$, and $S_6 = \alpha^{534}$. In the last step, $\deg[C^{(6)}(x)] = 1 = \nu$ so that $C^{(6)}(z) = (1 + \sigma_1 z) \cdot \sigma_0 = (1 + \alpha^{89}z) \cdot \alpha^{445} = (1 + Z_1 z) \cdot \alpha^{445}$. The root of $\sigma(z)$ is $Z_1 = \alpha^{-89} = \beta^{-1}$. Thus, the error polynomial is $e(x) = x^1$.

Case 2: Assume that there are two errors in the received vector and the error vector is $\boldsymbol{e}$ = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 0). Then the received vector is $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ = (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0) and its associated polynomial is $r(x) = x^{21} + x^{20} + x^{16} + x^{11} + x^9 + x^5 + x$. The syndromes are

$$S_i = r(\beta^i) = (\beta^i)^{21} + (\beta^i)^{20} + (\beta^i)^{16} + (\beta^i)^{11} + (\beta^i)^9 + (\beta^i)^5 + \beta^i,$$

where $i = 1, 2, 3, 4, 6$ and one has $S_1 = \alpha^{866}$, $S_2 = \alpha^{1732}$, $S_3 = \alpha^{620}$, $S_4 = \alpha^{1417}$, and $S_6 = \alpha^{1240}$.

If the number of errors is one, then, by Eqs. (27) and (9), the unknown syndrome is $S_5^{(1)} = \alpha^{236}$. Using the inverse-free BM algorithm, the computation terminates at step $k = 6$ and one obtains $C^{(6)}(x) = (\alpha^{620}x^3 + \alpha^{1732}x^2 + \alpha^{866}x + 1) \cdot \alpha^{113}$ from the consecutive known syndromes $S_1 = \alpha^{866}$, $S_2 = \alpha^{1732}$, $S_3 = \alpha^{620}$, $S_4 = \alpha^{1417}$, $S_5^{(1)} = \alpha^{236}$, and $S_6 = \alpha^{1240}$. In the last step, $\deg[C^{(6)}(x)] = 3 \neq 1 = \nu$ so that the assumption $\nu = 1$ is not valid. On the other hand, if the number of errors is two, then by Eqs. (28) and (9) the unknown syndrome is $S_5^{(2)} = \alpha^{1490}$. Then, using again the inverse-free BM algorithm, the computation terminates at step $k = 6$ and one obtains $C^{(6)}(x) = (\alpha^{267}x^2 + \alpha^{866}x + 1) \cdot \alpha^{1588}$ from the consecutively known syndromes $S_1 = \alpha^{866}$, $S_2 = \alpha^{1732}$, $S_3 = \alpha^{620}$, $S_4 = \alpha^{1417}$, $S_5^{(2)} = \alpha^{1490}$ and $S_6 = \alpha^{1240}$. In the last step, $\deg[C^{(6)}(x)] = 2 = \nu$ so that the error-locator polynomial $\sigma(z) = \alpha^{267}z^2 + \alpha^{886}z + 1$ is obtained. The roots of $\sigma(z)$ are $\beta^{-1} = \alpha^{-89}$ and $\beta^{-2} = \alpha^{-178}$ which implies the error polynomial is $e(x) = x^2 + x$.

Case 3: Assume that there are 3 errors in the received vector and the error vector is $\boldsymbol{e}$ = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 0). Then the received vector is $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ = (0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 1, 0, 1, 0, 1, 0) and its associated polynomial is $r(x) = x^{21} + x^{20} + x^{16} + x^{11} + x^9 + x^5 + x^3 + x$. The syndromes are

$$S_i = r(\beta^i) = (\beta^i)^{21} + (\beta^i)^{20} + (\beta^i)^{16} + (\beta^i)^{11} + (\beta^i)^9 + (\beta^i)^5 + (\beta^i)^3 + \beta^i,$$

where $i = 1, 2, 3, 4, 6$ and one has $S_1 = \alpha^{1712}$, $S_2 = \alpha^{1377}$, $S_3 = \alpha^{214}$, $S_4 = \alpha^{707}$, and $S_6 = \alpha^{428}$.

If the number of errors is one, then, by Eqs. (27) and (9), the unknown syndrome is $S_5^{(1)} = \alpha^{372}$. Uing the inverse-free BM algorithm, the computation terminates at step $k = 6$, $C^{(6)}(x) = (\alpha^{214}x^3 + \alpha^{1377}x^2 + \alpha^{1712}x + 1) \cdot \alpha^{1825}$ is obtained from the six consecutive known syndromes $S_1 = \alpha^{1712}$, $S_2 = \alpha^{1377}$, $S_3 = \alpha^{214}$, $S_4 = \alpha^{707}$, $S_5^{(1)} = \alpha^{372}$, and $S_6 = \alpha^{428}$. In the last step, the $\deg[C^{(6)}(x)] = 3 \neq 1 = \nu$ so that the assumption is not valid. When the

number of errors is two, by Eqs. (28) and (9), the unknown syndrome is $S_5^{(2)} = \alpha^{431}$. Using the inverse-free BM algorithm, the error-locator polynomial $C^{(6)}(x) = (\alpha^{607}x^3 + \alpha^{2030}x^2 + \alpha^{1712}x + 1) \cdot \alpha^{171}$ is obtained at step $k = 6$ from the six consecutive known syndromes $S_1 = \alpha^{1712}$, $S_2 = \alpha^{1377}$, $S_3 = \alpha^{214}$, $S_4 = \alpha^{707}$, $S_5^{(2)} = \alpha^{431}$, and $S_6 = \alpha^{428}$. In the last step, $\deg[C^{(6)}(x)] = 3 \neq 2 = v$ so that the assumption again is also not valid. If the number of errors is three, then, by Eqs. (29) and (9), the unknown syndrome is $S_5^{(3)} = \alpha^{810}$. With these six consecutive known syndromes $S_1 = \alpha^{1712}$, $S_2 = \alpha^{1377}$, $S_3 = \alpha^{214}$, $S_4 = \alpha^{707}$, $S_5^{(3)} = \alpha^{810}$, and $S_6 = \alpha^{428}$, $C^{(6)}(x) = (\alpha^{534}x^3 + \alpha^{1890}x^2 + \alpha^{1712}x + 1) \cdot \alpha^{98}$ is obtained at step $k = 6$ by using the inverse-free BM algorithm. In the last step, the degree of $C^{(6)}(x)$ is 3 which equals to the number of errors v. Consequently, the error-locator polynomial $\sigma(z)$ equals $(\alpha^{534}z^3 + \alpha^{1890}z^2 + \alpha^{1712}z + 1) \cdot \alpha^{98}$ and applying the Chien-search method, the roots of $\sigma(z)$ are $\beta^{-1} = \alpha^{-89}$, $\beta^{-2} = \alpha^{-178}$, and $\beta^{-3} = \alpha^{-267}$, which implies finally that $e(x) = x^3 + x^2 + x$.

To decode the (47, 24, 11) QR code, first, let $S_k^{(v)}$ denote the unknown syndrome which is computed from v errors that occur in the received vector, where $k \in \{1, 2, \ldots, 10\}$ and $v \in \{1, 2, 3, 4, 5\}$. Then one can construct the needed consecutive syndromes S_1, S_2, S_3, S_4, $S_5^{(v)}$, S_6, S_7, S_8, S_9, $S_{10}^{(v)}$ for the inverse-free BM algorithm.

As in the above illustrative example of the (23, 12, 7) QR or Golay code the decoder for the (47, 24, 11) QR code also can be developed by the inverse-free BM algorithm to find the error-locator polynomial. This algorithm is summarized by the following seven steps:

(a) Initialize by letting $v = 1$.
(b) Compute the known syndromes S_1, S_2, S_3, S_4, S_5, S_6, S_7, S_8, S_9 from Eq. (3).
(c) Compute the two unknown syndromes $S_5^{(v)}, S_{10}^{(v)}$ for $1 \leq v \leq 5$ from the algorithm developed in section 3.1.
(d) Compute the error-locator polynomial $\sigma(z)$ from the consecutive known syndromes S_1, $S_2, S_3, S_4, S_5^{(v)}, S_6, S_7, S_8, S_9, S_{10}^{(v)}$ for v errors, using the inverse-free BM algorithm.
(e) If $\deg[\sigma(z)] = v$ go to step (g). Otherwise set $v = v + 1$.
(f) If $v > t$, stop. Otherwise, go to step (c).
(g) 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.

The above the decoding scheme has been verified exhaustively for t errors, $0 \leq t \leq 5$, by a software simulation. The method in section 3.1 for finding the unknown syndromes to complete the syndrome list makes it possible to apply the efficient inverse-free BM algorithm for decoding the QR code. Thus this new decoding scheme is suitable for both software and hardware realizations.

4. CONCLUSIONS

The widely used BM algorithm was originally developed to decode 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 algo-

rithm 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 specifically for the Golay and (47, 24, 11) QR codes, they can be extended to every QR code with irreducible generating polynomial, and possibly to every cyclic code. To make certain that in [13] new decoding method works successfully for the Golay and (47, 24, 11) QR codes, a C++ program is written and every error pattern is run for all possible errors. The result is that this decoding algorithm is shown for the (47, 24, 11) QR code to correct all cases of 5 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 (47, 24, 11) QR code found in [1] previously by part of the authors of the present paper.

REFERENCES

1. E. Prange, "Cyclic error-correcting codes in two symbols," Air Force Cambridge Research Center-TN-57-103, Cambridge, MA, 1957.
2. X. Chen, I. S. Reed, and T. K. Truong, "A performance comparison of the binary quadratic residue codes with the 1/2-rate convolutional codes," *IEEE Transactions on Information Theory*, Vol. 40, 1994, pp. 126-136.
3. R. He, I. S. Reed, T. K. Truong, and X Chen, "Decoding the (47, 24, 11) quadratic residue code," *IEEE Transactions on Information Theory*, Vol. 47, 2001, pp. 1181-1186.
4. I. S. Reed, X. Yin, and T. K. Truong, "Algebraic decoding of the (32, 16, 8) quadratic residue code," *IEEE Transactions on Information Theory*, Vol. IT-36, 1990, pp. 876-880.
5. I. S. Reed, T. K. Truong, X. Chen, and X. Yin, "Algebraic decoding of the (41, 21, 9) quadratic residue code," *IEEE Transactions on Information Theory*, Vol. IT-38, 1992, pp. 974-986.
6. X. Chen, I. S. Reed, and T. K. Truong, "Decoding the (73, 37, 13) quadratic residue code," in *Proceedings of the IEE*, Vol. 141, 1994, pp. 253-258.
7. M. Elia, "Decoding of the (23, 12, 7) Golay code," *IEEE Transactions on Information Theory*, Vol. IT-33, 1987, pp. 150-151.
8. I. S. Reed and X. Chen, *Error-Control Coding for Data Networks*, Kluwer Academic publishers, Boston, 1999.
9. R. E. Berlekamp, *Algebraic Decoding Theory*, Mc-Graw Hill Publishers, New York, 1968.
10. J. L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Transactions on Information Theory*, Vol. IT-15, 1969, pp. 122-127.
11. I. M. Duursma and R. Kotter, "Error-locating pairs for cyclic codes," *IEEE Transactions on Information Theory*, Vol. IT-40, 1994, pp. 1108-1121.
12. I. S. Reed, M. T. Shih, and T. K. Troung, "VLSI design of inverse-free Berlekamp-

Massey algorithm," in *Proceedings of the IEE*, 1991, Vol. 138, pp. 295-298.
13. 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 Transactions on Communications*, Vol. 51, 2003, pp. 1463-1473.

APPENDIX

Proof: Theorem 1

(1) Let $I = \{i_1, i_2, \ldots, i_{v+1}\}$ and $J = \{j_1, j_2, \ldots, j_{v+1}\}$. Define the two matrices $X(I)$ and $X(J)$ as follows:

$$X(I) = \begin{bmatrix} Z_1^{i_1} & Z_2^{i_1} & \cdots & Z_v^{i_1} \\ Z_1^{i_2} & Z_2^{i_2} & \cdots & Z_v^{i_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{i_v} & Z_2^{i_v} & \cdots & Z_v^{i_v} \\ Z_1^{i_{v+1}} & Z_2^{i_{v+1}} & \cdots & Z_v^{i_{v+1}} \end{bmatrix}, \; X(J) = \begin{bmatrix} Z_1^{j_1} & Z_2^{j_1} & \cdots & Z_v^{j_1} \\ Z_1^{j_2} & Z_2^{j_2} & \cdots & Z_v^{j_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{j_v} & Z_2^{j_v} & \cdots & Z_v^{j_v} \\ Z_1^{j_{v+1}} & Z_2^{j_{v+1}} & \cdots & Z_v^{j_{v+1}} \end{bmatrix}.$$

Since $S(I, J) = X(I)X(J)^T$, the (r, s)th entry of $S(I, J)$ equals the inner product of the rth row vector of $X(I)$ and the sth column vector of $X(J)^T$ which is

$$(Z_1^{i_r}, Z_2^{i_r}, \ldots, Z_v^{i_r}) \cdot (Z_1^{j_s}, Z_2^{j_s}, \ldots, Z_v^{j_s}) = Z_1^{i_r + j_s} + Z_2^{i_r + j_s} + \ldots + Z_v^{i_r + j_s} = S_{i_r + j_s},$$

so that the (r, s)th entry of $S(I, J)$ is $S_{i_r + j_s}$.

Next, since $Z_i^l = \beta^{r_i \cdot l}$, if $l \equiv l' \bmod n$, then $r_i \cdot l \equiv r_j \cdot l' \bmod n$, *i.e.* $Z_i^l = \beta^{r_i \cdot l} = \beta^{r_i \cdot l'} = (\beta^{r_i})^{l'} = Z_i^{l'}$. Hence $S_k = Z_1^l + Z_2^l + \ldots + Z_v^l = Z_1^{l'} + Z_2^{l'} + \ldots + Z_v^{l'} = S_{l'}$, if $l \equiv l' \bmod n$; that is, the summation of the indices of the entries in $S(I, J)$ is modulo n.

(2) To prove Eq. (8b), since $S(I, J)$ is a product of two matrices whose ranks are both less than $v + 1$, the rank of $S(I, J)$ is also less than $v + 1$. Hence the determinant of $S(I, J)$ is zero, *i.e.*, $\det(S(I, J)) = 0$.

Proof: Theorem 2

Let $u = v + 1$ and let

$$S(I, J) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1u} \\ a_{21} & a_{22} & \cdots & a_{2u} \\ \vdots & \vdots & \ddots & \vdots \\ a_{u1} & a_{u2} & \cdots & a_{uu} \end{bmatrix} = (A_1, A_2, \ldots, A_u),$$

where $(A_1, A_2, \ldots, A_u)$ are the column vectors of $S(I, J)$.

If the unknown syndrome S_r is the (i, j)th entry of $S(I, J)$, *i.e.* $a_{i,j} = S_r$, then the jth column vector of $S(I, J)$ can be expressed as a sum of two vectors as follows:

$$\begin{aligned} A_j &= [a_{i,j} \quad \cdots \quad a_{i-1,j} \quad S_r \quad a_{i+1,j} \quad \cdots \quad a_{u,j}]^T \\ &= [a_{i,j} \quad \cdots \quad a_{i-1,j} \quad 0 \quad a_{i+1,j} \quad \cdots \quad a_{u,j}]^T + [0 \quad \cdots \quad 0 \quad S_r \quad 0 \quad \cdots \quad 0]^T \\ &= A_j^0 + A_j^c. \end{aligned}$$

Hence, from a basic property of determinants, one has

$$\begin{aligned} &\det(S(I,J)) = \det(A_1,\ldots,A_{j-1},A_j,A_{j+1},\ldots,A_u) = \det(A_1,\ldots,A_{j-1},A_j^0+A_j^c,A_{j+1},\ldots,A_u) \\ &= \det(A_1,\ldots,A_{j-1},A_j^0,A_{j+1},\ldots,A_u) + \det(A_1,\ldots,A_{j-1},A_j^c,A_{j+1},\ldots,A_u), \end{aligned}$$

i.e.

$$\det(S(I,J)) = \begin{vmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \cdots & a_{1,u} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & \cdots & a_{i-1,u} \\ a_{i,1} & \cdots & a_{i,j-1} & 0 & a_{i,j+1} & \cdots & a_{i,u} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & \cdots & a_{i+1,u} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{u,1} & \cdots & a_{u,j-1} & a_{u,j} & a_{u,j+1} & \cdots & a_{u,u} \end{vmatrix} +$$

$$\begin{vmatrix} a_{1,1} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1,u} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \cdots & a_{i-1,u} \\ a_{i,1} & \cdots & a_{i,j-1} & S_r & a_{i,j+1} & \cdots & a_{i,u} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \cdots & a_{i+1,u} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{u,1} & \cdots & a_{u,j-1} & 0 & a_{u,j+1} & \cdots & a_{u,u} \end{vmatrix}.$$

The matrix of the first determinant in the right-hand side is the same as $S(I, J)$ except for the (i, j)th position which is 0. The second determinant is

$$\det(A_1,\ldots,A_{j-1},A_j^c,A_{j+1},\ldots,A_u) = \begin{vmatrix} a_{1,1} & \cdots & a_{1,j-1} & 0 & a_{1,j+1} & \cdots & a_{1,u} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \cdots & a_{i-1,u} \\ a_{i,1} & \cdots & a_{i,j-1} & S_r & a_{i,j+1} & \cdots & a_{i,u} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \cdots & a_{i+1,u} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{u,1} & \cdots & a_{u,j-1} & 0 & a_{u,j+1} & \cdots & a_{u,u} \end{vmatrix}$$

$$= S_r \cdot \begin{vmatrix} a_{1,1} & \cdots & a_{1,j-1} & a_{1,j+1} & \cdots & a_{1,u} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{i-1,1} & \cdots & a_{i-1,j-1} & a_{i-1,j+1} & \cdots & a_{i-1,u} \\ a_{i+1,1} & \cdots & a_{i+1,j-1} & a_{i+1,j+1} & \cdots & a_{i+1,u} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{u,1} & \cdots & a_{u,j-1} & a_{u,j+1} & \cdots & a_{u,u} \end{vmatrix} = S_r \cdot \det(\Delta).$$

One has $\det(S(I, J)) = \det(\Delta_0) + S_r \cdot \det(\Delta)$ where Δ_0 is the matrix of the first determinant of the right hand side of above equation for $\det(S(I, J))$. Since $\det(S(I, J)) = 0$, and the characteristic of the field is 2, one has $S_r \cdot \det(\Delta) = \det(\Delta_0)$. Thus, $S_r = \det(\Delta_0)/\det(\Delta)$.

Proof: The Algorithm 1 in section 2

Let QR code with length n and $Q = Q_n \cup \{0, r\}$. What we are looking for is a pair of $(v + 1)$-sets $I, J \subset Q$ such that among the entries of $u = v + 1$, there is exactly one unknown syndrome S_r (which appeared only once) and all others are either known syndromes or S_0.

From (8a), the set of sub-indices of entries S_i's in the matrix $u = v + 1$ is

$$\{i_1 + j_1, i_1 + j_2, \ldots, i_1 + j_{v+1}, i_2 + j_1, i_2 + j_2, \ldots, i_2 + j_{v+1}, \ldots, i_{v+1} + j_1, i_{v+1} + j_2, \ldots, i_{v+1} + j_{v+1}\}^*,$$

where the * means that this set is a multi-set. The multi-set described above is, by definition, equal to the multi-set $I \oplus J = \{(i + j) \bmod n \mid i \in I, j \in J\}^*$. Therefore, it suffers to find $I, J \subset Q$ such that $I \oplus J$ contains exactly one r and all other elements are in Q, *i.e.* $(I \oplus J) - \{r\} \subset Q$.

If $I = \{i_1, \ldots, i_{v+1}\}$ and $J = \{j_1, \ldots, j_{v+1}\}$ are two subsets of Q and each contains $v + 1$ distinct elements, then by definition for each $i \in I$, $\{i\} \oplus J = \{(i + j) \bmod n \mid j \in J\}^*$. Since J has no repeated element, *i.e.* $j_1, \ldots, j_{v+1}$ are all distinct, $\{i\} \oplus J$ has no repeated element as well. Hence, the multi-set $\{i\} \oplus J$ is just the "ordinary" sum of the element $i \in Q$ and the subset $J \subset Q$, which is $i + J = \{(i + j) \bmod n \mid j \in J\}$. That is, for each $i \in I$, one has $\{i\} \oplus J = i + J$. Now, the multi-set $I \oplus J$ is

$$\begin{aligned}
&\{i_1 + j_1, \ldots, i_1 + j_{v+1}, i_2 + j_1, \ldots, i_2 + j_{v+1}, \ldots, i_{v+1} + j_1, \ldots\} \\
&= \{i_1 + j_1, \ldots, i_1 + j_{v+1}\} \cup \{i_2 + j_1, \ldots, i_2 + j_{v+1}\} \cup \ldots \cup \{i_{v+1} + j_1, \ldots, i_{v+1} + j_{v+1}\} \\
&= (i_1 + J) \bigcup (i_2 + J) \cup \ldots \cup (i_{v+1} + J) = \bigcup_{i \in I} (i + J).
\end{aligned}$$

Hence, if $I \oplus J \subset Q$, then $\bigcup_{i \in I} i + J \subset Q$ and one has, for each $i \in I$, that $i + J \subset Q$. This implies $J \subset Q - i$ for each $i \in I$, and therefore $J \subset \bigcap_{i \in I} Q - i$.

Conversely, if $J \subset \bigcap_{i \in I} Q - i$, then for each $i \in I$, $J \subset Q - i$, which yields $i + j \subset Q$ for each $i \in I$. This implies that $I \oplus J = \bigcup_{i \in I} (i + J) \subset Q$.

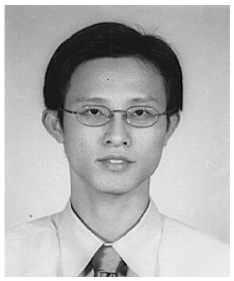
In summary, one has $I \oplus J \subset Q$ if and only if $J \subset \bigcap_{i \in I} (Q - i)$. From the discussion above, to find a pair of $(v + 1)$-subsets I, J of Q such that $I \oplus J \subset Q$ is equivalent to find a $(v + 1)$-subset $I = \{i_1, \ldots, i_{v+1}\}$ of Q satisfying the condition that the intersection $\bigcap_{i \in I} (Q - i) = (Q - i_1) \cap \ldots \cap (Q - i_{v+1})$ contains more than $v + 1$ elements. If this is the case, J can be taken to be any $(v + 1)$-subset of $\bigcap_{i \in I} (Q - i)$, *i.e.* $J \subset \bigcap_{i \in I} (Q - i)$, and consequently one has the desired condition $I \oplus J \subset Q$.

Moreover, if the multi-set $I \oplus J$ contains only one r, then there is exactly one S_r in the matrix $S(I, J)$. This completes the proof.

Yan-Haw Chen (陳延華) was born in Taipei, Taiwan, in 1967. He received the B.Eng. and M.Eng. degrees in Information Engineering from I-Shou University, Kaohsiung, Taiwan, in 1997 and 1999, respectively, and the Ph.D. degree in Electrical from I-Shou University, Kaohsiung, Taiwan, in 2006. In Feb. 2006, he joined the Fortune Institute of Technology, where he is now an Assistant Professor in the Department of Computer Science and Information Engineering. His research interests include error-correcting code, VLSI architecture design and communication systems.

Trieu-Kien Truong (張肇健) was born in Vietnam on December 4, 1944. He received the B.S. degree from National Cheng Kung University, Taiwan, in 1967, the M.S. degree from Washington University, St Louis, MO, in 1971, and the Ph.D. degree from the University of Southern California, LA, CA, in 1976, all in Electrical Engineering. From 1975 to 1992, he was a Senior Member of Technical Staff (E6) in the Communication System Research Section of the JPL, Pasadena, CA. Currently, he is a Chair Professor and the Dean of collage of Electrical and Information Engineering, I-Shou University, Taiwan. His research interests include error-correcting code, VLSI architecture design, communication systems, signal processing, and image compression. He served as an Editor in the Asia area for the Journal of Visual Communication and Image Representation and as an Editor in the area of Coding Theory & Techniques for the IEEE Transactions on Communications.

Yaotsu Chang (張耀祖) received the B.S. degree in Mathematics from Soochow University, Taipei, Taiwan, R.O.C., and the M.S. degree in Mathematics from National Tsing Hua University, Hsinchu, Taiwan, R.O.C., and the Ph.D. degree in Mathematics from the University of Michigan, Ann Arbor, in 1994. He is a Professor in the Department of Applied Mathematics, I-Shou University, Kaohsiung, Taiwan, R.O.C. His research interests include error-correcting code, finite field, and algebraic combinatorics.



C. D. Lee (李崇道) was born in Taipei, Taiwan, R.O.C., in 1978. He received the B.S. degree in Applied Mathematics and the M.E. degree in Information Engineering from I-Shou Univrsity, Kaohsiung, Taiwan, R.O.C., in 1999 and 2001, respectively, and the Ph.D. degree in Information Engineering from I-Shou University, Kaohsiung, Taiwan, in 2006.

Shi-Huang Chen (陳璽煌) was born in Tainan, Taiwan, R.O.C. in 1972. He received his B.Eng. and M.Eng. degrees from the Kaohsiung Polytechnic Institute, Kaohsiung, Taiwan, in 1994 and 1996, respectively, and the Ph.D. degree from the National Cheng Kung University, Tainan, Taiwan, in 2002, all in Electrical Engineering. Between 2001 and 2003, he was a research engineer at the AVXing Inc., Kaohsiung, Taiwan. He also worked as an adjunct lecturer in the Department of Information Engineering at the I-Shou University from Feb. 1998 to June 2002. In Feb. 2003, he joined the Shu-Te University, where he is now an Assistant Professor in the Department of Computer Science and Information Engineering. His research interests include wavelet transform, speech/audio processing, video coding, and multimedia communication standards. Dr. Chen is a member of IEEE.