

Short Paper

Decoding Binary Quadratic Residue Codes Using the Euclidean Algorithm*

PEI-YU SHIH, WEN-KU SU, TRIEU-KIEN TRUONG AND YAOTSU CHANG*

Department of Information Engineering

**Department of Applied Mathematics*

I-Shou University

Kaohsiung, 840 Taiwan

A simplified algorithm for decoding binary quadratic residue (QR) codes is developed in this paper. The key idea is to use the efficient Euclidean algorithm to determine the greatest common divisor of two specific polynomials which can be shown to be the error-locator polynomial. This proposed technique differs from the previous schemes developed for QR codes. It is especially simple due to the well-developed Euclidean algorithm. In this paper, an example using the proposed algorithm to decode the (41, 21, 9) quadratic residue code is given and a C++ program of the proposed algorithm has been executed successfully to run all correctable error patterns. The simulations of this new algorithm compared with the Berlekamp-Massey (BM) algorithm for the (71, 36, 11) and (79, 40, 15) quadratic residue codes are shown.

Keywords: quadratic residue code, the euclidean algorithm, unknown syndromes, known syndromes, syndrome polynomial, error-locator polynomial, the Chien search

1. INTRODUCTION

The error correcting codes can be used to improve performance in variety of applications including the spacecraft, satellite communication system [1], CD [2], HDTV [3], and DVD [4]. In 1958, Prange [5] introduced QR codes which are cyclic codes with high error-correcting capacity. These binary QR codes have code rates greater than or equal to 1/2 and generally have large minimum distance. Most of the binary QR codes are the best known codes, such as the famous Hamming code [6] and Golay code [7-9].

In the past decades, the methods used most often to decode binary QR codes include the Sylvester resultant [10, 11] and Gröbner bases [12, 13] methods. These methods can be used to solve the Newton identities that are non-linear, multivariate equations of quite high degrees. It becomes very difficult when the code length becomes large. However, it has difficulty for hardware implementation. Recently, He *et al.* [14] presented a technique to express the unknown syndromes as functions of the known syndromes and made use of this technique to decode binary (47, 24, 11) QR code up to the

Received August 2, 2007; revised December 10, 2007; accepted March 13, 2008.

Communicated by Chi-Jen Lu.

* This work was presented in part at the proceedings of the International Computer Symposium, 2006, Taipei, Taiwan, and supported by the National Science Council of Taiwan, R.O.C., under grants No. NSC 95-2221-E-214-042 and NSC 96-2221-E-214.

five errors. More recently, the authors [15, 16] used the technique mentioned above to obtain enough consecutive syndromes in binary QR codes of lengths 71, 79, 97, 103, and 113. Then the error-locator polynomial is found by using the inverse-free Berlekamp-Massey (BM) algorithm. Until now, the QR codes of lengths less than or equal to 113 have been decoded except for the case of length 89.

In this paper, a new decoding scheme to decode binary QR codes is proposed. It is based on the Euclidean algorithm which is an efficient method to find the error-locator polynomial in Reed-Solomon (RS) and Bose-Chaudhuri-Hocquenghem (BCH) decoders. Even though the code rates of QR codes are approximately $1/2$ and many QR codes are better than BCH codes with the code length n and dimension k , see Fig. 5.2 of [17], the proposed decoders for QR codes cost more computational complexity than the decoders for BCH codes by using the Euclidean algorithm. Therefore, an efficient decoding algorithm needs to be developed for QR codes.

The proposed decoding scheme has been verified by software simulation using programs written in C++ language. An exhaustive computer simulation running every error patterns within error-correcting capacity was executed successfully for the (23, 12, 7), (41, 21, 9), (47, 24, 11), and (71, 36, 11) QR codes. However, the computer search for the error patterns of the (79, 40, 15), (97, 49, 15), and (103, 52, 19) QR codes are not exhaustive. In other words, approximate one hundred million error patterns had been checked successfully and, as a consequence, demonstrated from a computer simulation that the algorithm for decoding these QR codes works well.

This paper is organized as follows: A brief review of the binary QR codes and syndrome polynomial is introduced in sections 2 and 3, respectively. A new decoding algorithm for binary QR codes is proposed in section 4. An example to decode (41, 21, 9) QR code is illustrated in detail. A few short remarks and conclusions of the new decoding algorithm are given in section 5. The simulation results of the proposed algorithm and the BM algorithm are given in the last section of the paper.

2. TERMINOLOGY AND BACKGROUND OF QUADRATIC RESIDUE CODES

Let n be a prime number of the form $n \equiv \pm 1 \pmod{8}$. A binary QR code of length n is an $(n, (n+1)/2)$ cyclic code with the generator polynomial

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

where Q_n is the collection of all nonzero quadratic residues modulo n ; that is,

$$Q_n = \{i \mid i \equiv j^2 \pmod{n} \text{ for } 1 \leq j \leq n-1\} \quad (2)$$

and β is a primitive n th root of unity in the finite field $GF(2^m)$, where m is the smallest positive integer such that $n \mid 2^m - 1$.

Let the code polynomial $c(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$ be transmitted through a noisy channel. Then the received polynomial $r(x) = r_0 + r_1x + \dots + r_{n-1}x^{n-1}$ has the form

$$r(x) = c(x) + e(x), \tag{3}$$

where $e(x) = e_0 + e_1x + \dots + e_{n-1}x^{n-1}$ is an error polynomial.

Suppose that there are v errors occurred in the received polynomial $r(x)$. In other words, the error polynomial $e(x)$ has v nonzero terms, namely,

$$e(x) = x^{l_1} + x^{l_2} + \dots + x^{l_v} \tag{4}$$

where $0 \leq l_1 < l_2 < \dots < l_v \leq n - 1$.

The syndrome S_i is defined as

$$S_i = r(\beta^i) = c(\beta^i) + e(\beta^i). \tag{5}$$

The known syndromes can be obtained by evaluating $r(x)$ at the roots of $g(x)$. That is,

$$S_i = e(\beta^i) = (\beta^{l_1})^i + (\beta^{l_2})^i + \dots + (\beta^{l_v})^i, \quad i \in Q_n \tag{6}$$

where β^{l_j} for $1 \leq j \leq v$ are called the error locators. If i is not found in the set Q_n , the syndrome S_i is called the unknown syndrome. The error-locator polynomial $\sigma(x)$ with degree v can be expressed as

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

where $\sigma_1 = X_1 + \dots + X_v$, $\sigma_2 = X_1X_2 + \dots + X_{v-1}X_v$, ..., and $\sigma_v = X_1 \dots X_v$.

For a QR code with the minimum distance d , an error polynomial is said to be correctable if its weight is less than or equal to the error-correcting capacity $t = \lfloor (d - 1)/2 \rfloor$ where $\lfloor x \rfloor$ notes the greatest integer less than or equal to x .

For any binary cyclic codes, there is an obvious relation among syndromes, namely, $S_{2i} = S_i^2$, with indices modulo n , if necessary. Finally, let the syndrome polynomial $S(x)$ be defined as the polynomial

$$S(x) = S_1x + S_2x^2 + \dots + S_{n-1}x^{n-1}. \tag{8}$$

In order to obtain $S(x)$ defined above, all syndromes need to be found. However, only known syndromes can be calculated directly from $r(x)$. The unknown syndromes cannot be obtained by evaluating $r(x)$ at the roots of the generator polynomial $g(x)$. Since all unknown syndromes are some powers of specific unknown syndromes, called the primary unknown syndromes of the QR code, the values of all unknown syndromes can be obtained if the values of the primary unknown syndromes are determined.

The same procedure given in [15] can be used in this paper to express the needed primary unknown syndromes as functions of some certain known syndromes. Therefore, all of the unknown syndromes can be calculated once the values of the primary unknown syndromes are determined. The following is a brief review of the technique mentioned in [15].

Assume that v errors occur in the received word. Let $I = \{i_1, i_2, \dots, i_{v+1}\}$ and $J = \{j_1, j_2, \dots, j_{v+1}\}$ denote two subsets of $\{0, 1, 2, \dots, n - 1\}$, respectively. These index subsets

can be found by an explicit use of the fast algorithm developed in [15]. Next, consider the matrix $S(I, J)$ of size $(v + 1) \times (v + 1)$ as follows:

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

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

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

If there is only one unknown syndrome, say S_r , among the entries of $S(I, J)$, then S_r can be expressed as a function in terms of some known syndromes. Hence, during the decoding process, one is able to calculate the value of S_r with the information about those known syndromes. The complete procedures to determine the primary unknown syndromes for some QR codes are shown in [14-16]. In what follows, the polynomials $S(x)$ and $x^n - 1$ will be used in the proposed decoding scheme.

3. SYNDROME POLYNOMIAL

If the element β is a primitive root of $x^n - 1$, then $x^n - 1$ can be split into n linear factors, $(1 - \beta^i x)$, where $0 \leq i \leq n - 1$. It is straightforward to see that the all-one polynomial (AOP) $x^{n-1} + x^{n-2} + \dots + 1$ is equal to $\prod_{i=1}^{n-1} (1 - \beta^i x)$, i.e., $\beta^{-1} = \beta^{n-1}$, $\beta^{-2} = \beta^{n-2}$, ..., $\beta^{-(n-1)} = \beta^1$ are all the roots of the AOP. This fact leads to prove the following theorem.

Theorem 1 Let $c(x)$ and $e(x)$ be a codeword of a binary QR code of length n and a correctable error pattern of weight v , respectively. Also, let $S(x)$ given in Eq. (8) be the syndrome polynomial for the received codeword $r(x) = e(x) + c(x)$. If the weight of $e(x)$ is odd (resp., even), then $S(x)$ (resp., $1 + S(x)$) has v linear factors; that is, $(1 - \beta^i x)$, where β^{-i} belongs to $B = \{\beta^1, \beta^2, \dots, \beta^{n-1}\} = \{\beta^{-(n-1)}, \beta^{-(n-2)}, \dots, \beta^{-1}\}$.

Proof: Assume that the number of errors is odd, i.e., $v = 2u + 1$. By the definition of syndromes mentioned in section 2, we have $S_i = (\beta^{l_1})^i + (\beta^{l_2})^i + \dots + (\beta^{l_{2u+1}})^i$, where $0 \leq i \leq n - 1$. Then the evaluation of $S(x)$ at β^{-i} yields the following:

$$\begin{aligned} S(\beta^{-i}) &= (\beta^{l_1} + \beta^{l_2} + \dots + \beta^{l_{2u+1}})(\beta^{-i}) + (\beta^{2l_1} + \beta^{2l_2} + \dots + \beta^{2l_{2u+1}})(\beta^{-2i}) + \dots \\ &\quad + (\beta^{(n-1)l_1} + \beta^{(n-1)l_2} + \dots + \beta^{(n-1)l_{2u+1}})(\beta^{-(n-1)i}) \\ &= (\beta^{l_1-i} + \beta^{2(l_1-i)} + \dots + \beta^{(n-1)(l_1-i)}) + (\beta^{l_2-i} + \beta^{2(l_2-i)} + \dots + \beta^{(n-1)(l_2-i)}) + \dots \\ &\quad + (\beta^{l_{2u+1}-i} + \beta^{2(l_{2u+1}-i)} + \dots + \beta^{(n-1)(l_{2u+1}-i)}). \end{aligned} \tag{11}$$

Since each β^{-i} is a root of the AOP, $(\beta^{-i})^{n-1} + (\beta^{-i})^{n-2} + \dots + (\beta^{-i}) = 1$ is then obtained. In Eq. (11), if $i = l_j$, where $1 \leq j \leq 2u + 1$, then the j th summand equals $\beta^{l_j^{l_j}} + \beta^{2(l_j^{l_j})} + \dots + \beta^{(n-1)(l_j^{l_j})} = 1 + 1 + \dots + 1 = n - 1 \equiv 0 \pmod{2}$. All other summands have the same value $\beta^{l_j^{l_w}} + (\beta^{l_j^{l_w}})^2 + \dots + (\beta^{l_j^{l_w}})^{n-1} = 1$ for $w \neq j$ because $\beta^{l_j^{l_w}}$ is a root of AOP. Therefore, Eq. (11) becomes $S(\beta^{-i}) = 0 + 1 + \dots + 1 = 2u \equiv 0 \pmod{2}$ for $i = l_j$, where $1 \leq j \leq 2u + 1$. On the other hand, for $i \neq l_j$, then Eq. (11) becomes $S(\beta^{-i}) = 1 + 1 + \dots + 1 = 2u + 1 \equiv 1 \pmod{2}$. That is, for the case of odd errors, $S(x)$ has exactly v roots in B , *i.e.*, $\prod_{j=1}^v (1 - \beta^j x) \mid S(x)$, where $\prod_{j=1}^v (1 - \beta^j x)$ is the error-locator polynomial $\sigma(x)$. By a similar argument for the case of odd errors, when the number of errors is even, *i.e.*, $v = 2u$, one obtains $1 + S(\beta^i) = 1 + (2u - 1) \equiv 0 \pmod{2}$ for $i = l_j$ and $1 + S(\beta^{-i}) = 1 + 2u \equiv 1 \pmod{2} \neq 0$ for $i \neq l_j$, where $1 \leq j \leq 2u$. In other words, for the case of even errors, there are precisely v roots in B such that $1 + S(x) = 0$, *i.e.*, $\sigma(x) = \prod_{j=1}^v (1 - \beta^j x) \mid ((S(x) + 1))$. The proof of Theorem 1 is thus complete.

Recall that the polynomial $x^n - 1$ is equal to the product of the linear factors $(1 - \beta^i x)$, where $0 \leq i \leq n - 1$. Using this fact along with Theorem 1 implies that the greatest common divisor (*g.c.d.*) of $S(x)$ (*resp.*, $1 + S(x)$) and $x^n - 1$ is $\sigma(x)$ with degree v for $v \in \text{odd}$ (*resp.*, $v \in \text{even}$). It is well known that the Euclidean algorithm is an efficient method to determine the *g.c.d.* of two given polynomials. Based on this idea, a simplified algorithm is developed for decoding binary QR codes as shown in section 4.

4. DECODING OF QUADRATIC RESIDUE CODES

If the known syndromes calculated by Eq. (6) are all zeros, there is no error in the received word. When the errors occur in the received word, the decoding algorithm is composed of the following nine steps:

1. Compute the known syndromes for the QR code from Eq. (6).
2. Initialize by letting $v = 1$.
3. Compute the unknown syndromes of the QR code for v errors by applying the technique given in [14-16] and obtain the syndrome polynomial $S(x)$.
4. If v is odd (*resp.*, even), $P(x)$ is replaced by $S(x)$ (*resp.*, $1 + S(x)$).
5. Obtain *g.c.d.* $(x^n - 1, P(x))$ by using the Euclidean algorithm applied to $x^n - 1$ and $P(x)$.
6. If degree of *g.c.d.* $(x^n - 1, P(x))$ equals v , then the error-locator polynomial $\sigma(x)$ is equal to *g.c.d.* $(x^n - 1, P(x))$. Otherwise, set $v = v + 1$.
7. If $v > t$, stop. Otherwise, go to step 3.
8. Find the roots of $\sigma(x) = 0$ by the use of the Chien search.
9. The error pattern is determined and the received word is then corrected.

The decoding scheme developed here is shown in Fig. 1. The decoding algorithm written in C++ language have been executed to check possible error patterns of the binary QR codes with code lengths 23, 41, 47, 71, 79, 97, 103, respectively. A completely worked-out example of decoding binary (41, 21, 9) QR code up to four errors is given as follows:

Example: Let α be a root of the primitive polynomial $x^{20} + x^3 + 1$ and let $\beta = \alpha^{(2^{20}-1)/41} = \alpha^{25575}$ be a primitive 41st root of unity in $GF(2^{20})$. The set of quadratic residue modulo 41 defined in Eq. (2) is $Q_{41} = \{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\}$. According to Eq. (1), the generator polynomial of the binary (41, 21, 9) QR code can be written as

$$g(x) = \prod_{i \in Q_{41}} (x - \beta^i) \\ = 1 + x + x^3 + x^4 + x^6 + x^9 + x^{10} + x^{11} + x^{14} + x^{16} + x^{17} + x^{19} + x^{20}.$$

Assume the information polynomial is $I(x) = 1 + x^5 + x^9 + x^{10} + x^{14} + x^{15} + x^{16} + x^{19} + x^{20}$. Then the code polynomial $c(x)$, which is a multiple of $g(x)$, is

$$c(x) = 1 + x^2 + x^3 + x^7 + x^8 + x^9 + x^{15} + x^{16} + x^{19} + x^{22} + x^{24} + x^{26} + x^{28} \\ + x^{29} + x^{30} + x^{31} + x^{33} + x^{34} + x^{35} + x^{36} + x^{37} + x^{38} + x^{40}.$$

If the error polynomial $e(x)$ is assumed to be $x^1 + x^7 + x^{23} + x^{36}$, then the received polynomial is the sum of the code polynomial $c(x)$ and the error polynomial $e(x)$. That is,

$$r(x) = c(x) + e(x) = 1 + x + x^2 + x^3 + x^8 + x^9 + x^{15} + x^{16} + x^{19} + x^{22} + x^{23} + x^{24} \\ + x^{26} + x^{28} + x^{29} + x^{30} + x^{31} + x^{33} + x^{34} + x^{35} + x^{37} + x^{38} + x^{40}.$$

The decoding process developed in this paper is described as follows:

First of all, the known syndrome S_k for each k in Q_{41} can be calculated from the received polynomial $r(x)$. That is,

$$S_k = \prod_{i=0}^{40} r_i(\beta^k)^i, \quad k \in Q_{41}.$$

For the binary (41, 21, 9) QR code, every known syndromes (resp., unknown syndromes) can be expressed as some power of S_1 (resp., S_3). In other word, S_3 is the primary unknown syndrome of the (41, 21, 9) QR code. Therefore, the same procedure given in [15] can be used in this paper to define the value of the primary unknown syndrome for each hypothetic number of errors occurred. After the values of the primary syndromes S_1 and S_3 are determined, Table 1 shows the relations among syndromes for the (41, 21, 9) QR code.

By evaluating $r(x)$ at the roots of $g(x)$ mentioned above, the primary known syndrome is $S_1 = \alpha^{822540} \neq 0$, which means that there are errors occurred in the received polynomial $r(x)$.

If the number of errors is one, *i.e.*, $v = 1$, the primary unknown syndrome is $S_3 = S_1^3 = \alpha^{370470}$. After the determination of the primary syndromes S_1 and S_3 , all syndromes can also be determined. Therefore, the syndrome polynomial $S(x)$ is further obtained. The output of the Euclidean algorithm is

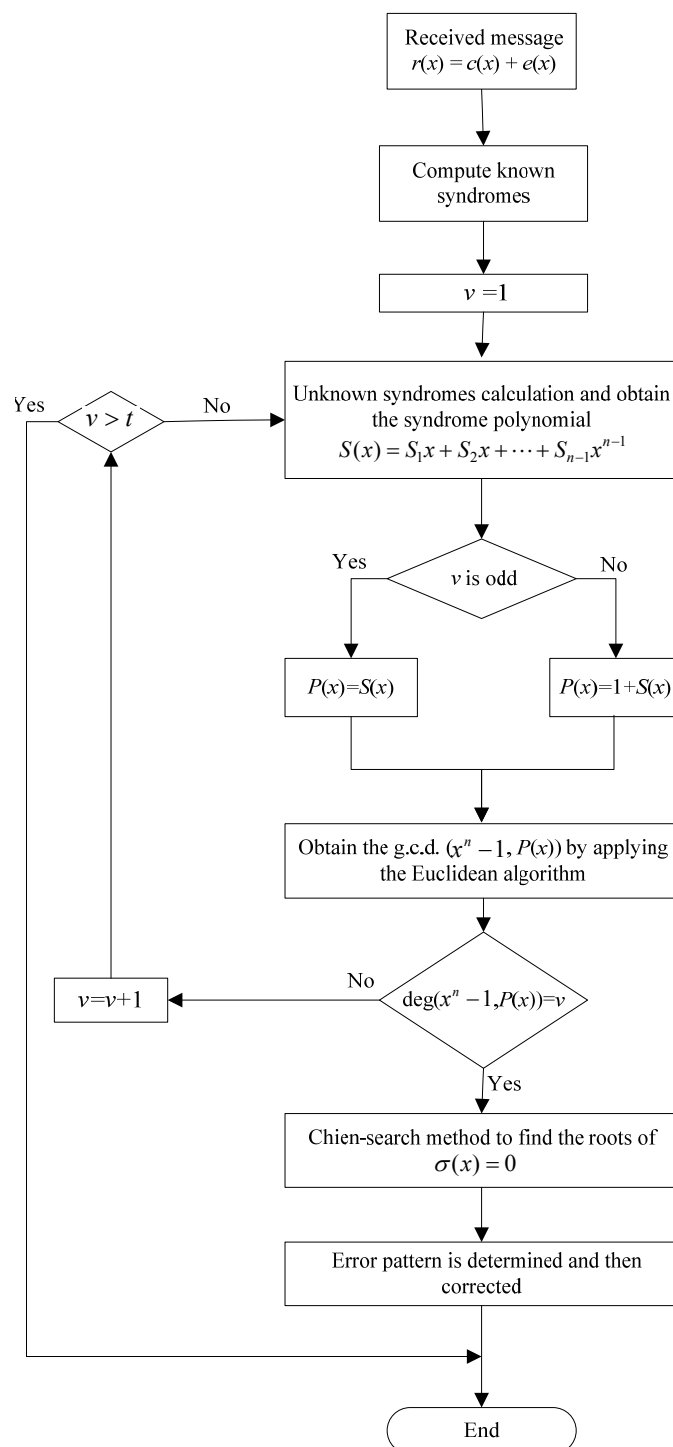


Fig. 1. Flowchart of the proposed QR decoder.

Table 1. Values of subindices “ t_i ” for identifies $S_{t_i} = S_j^{2^i}$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$j = 1$	2	4	8	16	32	23	5	10	20	40	39	37	33	25	9	18	36	31	21
$j = 3$	6	12	24	7	14	28	15	30	19	38	35	29	17	34	27	13	26	11	22

$$\begin{aligned} &\alpha^0 + \alpha^{822540}x + \alpha^{1006152}x^2 + \alpha^{780117}x^3 + \alpha^{60716}x^4 + \alpha^{415151}x^5 + \alpha^{431775}x^6 \\ &+ \alpha^{643571}x^7 + \alpha^{156564}x^8 + \alpha^{513338}x^9 + \alpha^{960279}x^{10} + \alpha^{274912}x^{11} + \alpha^{184888}x^{12} \\ &+ \alpha^{504021}x^{13} + \alpha^{15137}x^{14} + \alpha^{631236}x^{15} + \alpha^{766422}x^{16} + \alpha^{380625}x^{17} + \alpha^{134849}x^{18} \\ &+ \alpha^{359}x^{19} + \alpha^{567333}x^{20} + \alpha^{292098}x^{21} + \alpha^{1016910}x^{22} + \alpha^{741675}x^{23}. \end{aligned}$$

Thus, the assumption is not valid and let $v = v + 1 = 2$.

If $v = 2$, the primary unknown syndrome S_3 can be determined by the technique developed in [15]. A computer search is used to find the following matrix of size 3×3 :

$$\begin{bmatrix} S_0 & S_1 & S_8 \\ S_1 & S_2 & S_9 \\ S_2 & S_3 & S_{10} \end{bmatrix}.$$

There is only one unknown syndrome S_3 among the entries of this matrix. By [14], the determinant of the above matrix is zero. The unknown syndrome S_3 for the two-error case is

$$S_3 = \frac{S_1S_2S_9 + S_2^2S_8 + S_1^2S_{10}}{S_1S_8} = \alpha^{280675},$$

where $S_0 = 0$ and $S_1 = \alpha^{822584}$. Since $v = 2$ is even, the polynomial $1 + S(x)$ is used in Euclid’s algorithm. Simulation result shows that the output of the Euclidean algorithm is

$$\begin{aligned} &\alpha^0 + \alpha^{822540}x + \alpha^{429347}x^2 + \alpha^{175384}x^3 + \alpha^{91243}x^4 + \alpha^{377861}x^5 + \alpha^{214207}x^6 \\ &+ \alpha^{361581}x^7 + \alpha^{697654}x^8 + \alpha^{858679}x^9 + \alpha^{876804}x^{10} + \alpha^{103229}x^{11} + \alpha^{803475}x^{12} \\ &+ \alpha^{976871}x^{13} + \alpha^{394971}x^{14} + \alpha^{709321}x^{15} + \alpha^{445996}x^{16} + \alpha^{239844}x^{17} + \alpha^{323668}x^{18} \\ &+ \alpha^{133364}x^{19} + \alpha^{237532}x^{20} + \alpha^{414766}x^{21} + \alpha^{426278}x^{22} + \alpha^{403110}x^{23} + \alpha^{127875}x^{24}. \end{aligned}$$

Thus, the assumption is also not valid.

If $v = 3$, the primary unknown syndrome S_3 can be determined by the following equation:

$$\begin{vmatrix} S_0 & S_1 & S_2 & S_5 \\ S_{31} & S_{32} & S_{33} & S_{36} \\ S_{39} & S_{40} & S_0 & S_3 \\ S_{40} & S_0 & S_1 & S_4 \end{vmatrix} = 0, \tag{12}$$

where $S_0 = 1$ and $S_1 = \alpha^{822584}$.

The unknown syndrome S_3 for the three-error case is $S_3 = \alpha^{4619964}$. Because $v = 3$ is odd, the syndrome polynomial $S(x)$ is used in the Euclidean algorithm. Similarly, the output of the Euclidean algorithm is

$$\begin{aligned} &\alpha^0 + \alpha^{822540}x + \alpha^{51831}x^2 + \alpha^{43076}x^3 + \alpha^{705575}x^4 + \alpha^{610852}x^5 + \alpha^{287586}x^6 + \alpha^{922050}x^7 \\ &+ \alpha^{423495}x^8 + \alpha^{674130}x^9 + \alpha^{538425}x^{10} + \alpha^{963789}x^{11} + \alpha^{638473}x^{12} + \alpha^{117350}x^{13} \\ &+ \alpha^{781657}x^{14} + \alpha^{722919}x^{15} + \alpha^{351960}x^{16} + \alpha^{76725}x^{17} \end{aligned}$$

and therefore the assumption is not valid.

If $v = 4$, the primary unknown syndrome S_3 can be determined as follows:

$$\begin{vmatrix} S_0 & S_1 & S_{23} & S_{31} & S_{37} \\ S_2 & S_3 & S_{25} & S_{33} & S_{39} \\ S_8 & S_9 & S_{31} & S_{39} & S_4 \\ S_9 & S_{10} & S_{32} & S_{40} & S_5 \\ S_{20} & S_{21} & S_2 & S_{10} & S_{16} \end{vmatrix} = 0, \tag{13}$$

where $S_0 = 0$ and $S_1 = \alpha^{822584}$.

The unknown syndrome S_3 for the four-error case is $S_3 = \alpha^{739576}$. Since $v = 4$ is defined to be even, the polynomial $1 + S(x)$ is used in the Euclidean algorithm. Experiment results show that the *g.c.d.* of polynomials $x^n - 1$ and $1 + S(x)$ is $1 + \alpha^{822540}x + \alpha^{426775}x^2 + \alpha^{940185}x^3 + \alpha^{664950}x^4$ and its degree is equal to four. The error-locator polynomial is thus determined as

$$\sigma(x) = 1 + \alpha^{822540}x + \alpha^{426775}x^2 + \alpha^{940185}x^3 + \alpha^{664950}x^4.$$

There exist exactly four roots $\beta^{-1}, \beta^{-7}, \beta^{-23}, \beta^{-36}$ in $\sigma(x)$ via the Chien search. The error polynomial $e(x) = x^1 + x^7 + x^{23} + x^{36}$ is thus determined.

5. CONCLUSIONS

This paper presents a new decoding scheme to decode some binary QR codes. In this proposed method, the Euclidean algorithm is utilized to determine the error-locator polynomial for QR decoders efficiently. The results had been verified by software simulation which differs from algebraic decoding schemes developed in [15, 16]. This approach provides an alternative way to decode QR codes.

6. SIMULATION RESULTS

The simulation results of the new decoding algorithm and the BM algorithm show that the speed of our decoding algorithm is often slower than the BM algorithm for QR

codes. Because the most time-consuming usage in our decoding algorithm is the computation of $g.c.d. (x^n - 1, P(x))$ using the Euclidean algorithm, especially, when the number of actual errors is not equal to the number of hypothetical errors occurred. In order to compare the decoding algorithm developed in [10, 15] for the (71, 36, 11) and (79, 40, 15) QR codes, these two algorithms have been verified and implemented on the computer using C++ language. The computational times shown in Table 2 were averaged over 100 computations. Furthermore, one observes from Table 2 that the speed of the proposed algorithm is slower than and almost equal to that of the BM algorithm given in [15, 16] for the (71, 36, 11) QR code and (79, 40, 15) QR code, respectively. Therefore, one needs to modify this new algorithm for which it offers a significant advantage in terms of computational complexity.

Table 2. Computation time in seconds to decode QR codes.

(n, k, d) QR code	Errors	New algorithm	BM algorithm
(71, 36, 11) QR code	5	0.047	0.008
(79, 40, 15) QR code	7	0.483	0.5

ACKNOWLEDGMENT

The authors would like to express their deepest appreciation to the Editor and the referees for their valuable and useful comments that led to this paper.

REFERENCES

1. Telemetry Channel Coding, Recommendation for Space Data System Standard, CCSDS 101.0-B-3, *Blue Book*, 1992.
2. S. B. Wicker and V. K. Bhargava, *Reed-Solomon Codes and Their Applications*, IEEE Press, New Jersey, 1994.
3. C. Basile *et al.*, "The U.S. HDTV standard the grand alliance," *IEEE Spectrum*, Vol. 32, 1995, pp. 36-45.
4. DVD Specifications for Rewritable Disc (DVD-RAM) Part 1, *Physical Specifications*, Version 2.0, 1999.
5. E. Prange, "Some cyclic error-correcting codes with simple decoding algorithms," Air Force Cambridge Research Center-TN-58-156, Cambridge, MA, 1958.
6. R. W. Hamming, "Error detecting and error correcting codes," *Bell System Technical Journal*, Vol. 29, 1950, pp. 147-160.
7. M. J. E. Golay, "Notes on digital coding," in *Proceedings of the Institute of Electrical and Electronic Engineers*, Vol. 37, 1949, pp. 657.
8. I. S. Reed, X. Yin, T. K. Truong, and J. K. Holmes, "Decoding the (24, 12, 8) Golay code," *IEE Proceedings - Communications*, Vol. 137, 1990, pp. 202-206.
9. M. Elia, "Algebraic decoding of the (23, 12, 7) Golay code," *IEEE Transactions on Information Theory*, Vol. 33, 1987, pp. 150-151.
10. 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. 36, 1990, pp. 876-

- 880.
11. I. S. Reed, T. K. Truong, X. Chen, and X. Yin, "The algebraic decoding of the (41, 21, 9) quadratic residue code," *IEEE Transactions on Information Theory*, Vol. 38, 1992, pp. 974-985.
 12. X. Chen, I. S. Reed, T. Helleseth, and T. K. Truong, "Use of Gröbner bases to decode binary cyclic codes up to the true minimum distance," *IEEE Transactions on Information Theory*, Vol. 40, 1994, pp. 1654-1661.
 13. P. Loustau and E. V. York, "On the decoding of cyclic codes using Gröbner bases," *Applicable Algebra in Engineering, Communication and Computing*, Vol. 8, 1997, pp. 469-483.
 14. 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.
 15. 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.
 16. T. K. Truong, Y. Chang, Y. H. Chen, and C. D. Lee, "Algebraic decoding of (103, 52, 19), and (113, 57, 15) quadratic residue codes," *IEEE Transactions on Communications*, Vol. 53, 2005, pp. 749-754.
 17. R. E. Blahut, *Theory and Practice of Error Control Codes*, Addison-Wesley, MA, 1983.

Pei-Yu Shih (施沛渝) was born in Taipei, Taiwan, in 1976. She received the B.S. and M.S. degrees in Mathematics from Soochow University, Taipei, Taiwan, R.O.C., in 1999 and 2002, respectively, and is now working toward the Ph.D. degree at I-Shou University, Kaohsiung, Taiwan, R.O.C. Her research interests include error-correcting code and communication systems.

Wen-Ku Su (蘇文谷) was born in Taipei, Taiwan, in 1977. He received the B.S. and M.S. degrees in Mathematics from Soochow University, Taipei, Taiwan, R.O.C., in 2002 and 2005, respectively, and is now working toward the Ph.D. degree at I-Shou University, Kaohsiung, Taiwan, R.O.C. His research interests include error-correcting code 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 and Techniques for the IEEE Transactions on Communications. Dr. Truong is a Fellow of the IEEE.

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.