New algebraic decoding method for the (41, 21,9) quadratic residue code

Mohammed M. Al-Ashker[a], Ramez Al.Shorbassi[b]
[a]Department of Mathematics
Islamic University of Gaza, Palestine
[b]Ministry of education, Gaza, Palestine.
E-mail :*mashker@iugaza.edu.ps*(M.Al-Ashker),
*mathematic*2006@*hotmail.com*(R.Al-Shorbassi)

Abstract

In this paper, a decoding algorithm was given for the (41, 21, 9) binary QR code. Here, some new more general properties are found for the syndromes of the subclass of binary QR codes of length $n = 8l + 1$. Using these properties, the new theorems needed to decode this subclass of the QR codes are obtained and proved in [6]. 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). For the details about syndromes we refer the reader to [1]. A new algebraic decoding algorithm for the (41, 21, 9) binary QR code is presented.

AMS: Subject Classification 2000:94B15
Keywords: Cyclic codes, Newton identities, QR code.

1 Introduction

The class of quadratic residue QR codes was introduced by Prange in 1958 [9]. It is a nice family of cyclic codes and has approximately 1/2 code rates. In the past decades, most of decoding methods for the QR codes are used to solve the Newton identities that are nonlinear, multivariate equations of quite high degree. It becomes very difficult when the weight of the occurred error becomes large. Moreover, different QR codes use different sets of conditions to determine the error locations. As a result, it is not practical for software implementation. The Lookup Table Decoding algorithm named (LTD) algorithm given in [3] to decode the binary systematic $(41, 21, 9)$ QR code up to 4 errors. Such an algorithm determines directly the error locations by lookup tables without the operations of multiplication over a finite field.
The Lagrange interpolation formula presented in [4] to determine the error check and error locator polynomials for the use of decoding algorithm of the $(41, 21, 9)$ QR code.
The finite field version of Lagrange interpolation formula is as follows: for $q \geq 0$ let a_0, a_1, ..., a_q be $q+1$ distinct elements of $\mathbb{E}$, and let b_0, b_1, ..., b_q be $q+1$ arbitrary elements of $\mathbb{E}$. Then there exists exactly one polynomial $L(a_i) = b_i$ for $i = 0, 1, \ldots, q$. The polynomial $L(x)$ can be written in the form

$$L(x) = \sum_{i=0}^{q} \frac{b_i}{h'(a_i)} \frac{h(x)}{x - a_i}$$

with $h(x) = \prod_{k=0}^{q}(x - a_k)$ and $h'(x)$ is the derivative of $h(x)$.

In this paper, a new technique is found to have the unknown syndrome S_3 by Maple 13 which is a necessary condition for decoding the (41, 21, 9) QR code.

2 Background of the (41, 21, 9) QR code

A binary QR code of length n is an (n, (n+1)/2) cyclic code over $GF(2^m)$ with generator polynomial g(x) where m is some integer. The

length of this code is a prime number of the form $n = 8l + 1$ where l is some integer. The generator polynomial $g(x)$ is defined by

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

where β is a primitive nth root of unity in the finite field $GF(2^m)$ with m being the smallest positive integer such that $n|2^m - 1$ and Q_n is the collection of all nonzero quadratic residues modulo n given by

$$Q_n = \{i | i \equiv j^2 \ mod \ n \ for \ 1 \leq j \leq n - 1\}. \tag{2}$$

For the (41, 21, 9) QR code, the set of quadratic residue modulo 41, is

$$Q_{41} = \{1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40\}.$$

See [8]. The smallest extension field of F_2 is $F_{2^{20}}$. Let α be a root of the primitive polynomial $f(x) = x^{20} + x^3 + 1$, using **Maple 13** to have $f(x)$ is irreducible over F_2 and let $\beta = \alpha^{(2^m-1)/n} = \alpha^{(2^{20}-1)/41} = \alpha^{25575}$ be a primitive 41^{st} root of unity in $GF(2^{20})$. The generator polynomial of binary (41,21, 9) QR code can be written as

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

Let a codeword $c(x) = m(x)g(x)$ be transmitted through a noisy channel to obtain a received codeword of the form $r(x) = c(x) + e(x) = \sum_{i=1}^{40} c_i x^i + \sum_{i=1}^{40} e_i x^i$, where e(x) is the polynomial of the received error pattern vector. The syndromes S_i are defined by

$$S_i = r(\beta^i) = e(\beta^i), \quad for \ i \in Q_{41}. \tag{3}$$

Otherwise, the syndromes are called the unknown syndromes and are not obtained directly.

The aim of decoding is to find the ν unknown error locations from the known syndromes S_i for $i \in Q$. For this purpose the error-locator polynomial $L(z)$ for every correctable error pattern is defined by

$$L(z) = \prod_{i=1}^{\nu} (z - Z_i) = z^\nu + \sum_{j=1}^{\nu} \sigma_j z^{\nu - j}. \tag{4}$$

Here, Z_j for $1 \leq j \leq \nu$ are the locations of the ν errors, i.e. $Z_j = \alpha^{r_j}$, where r_j locates the position of the error to be corrected and $\nu < t$.

3 Important theorem to decode the (41, 21, 9) QR code

To decode a QR code it suffices to find the error-locator polynomial $L(z)$. It is well known that S_i and σ_j are related by the following Newton identities [7]

$$S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + \sigma_j = 0 \quad (1 \leq i \leq \nu, i = odd)$$

$$S_i + \sum_{j=1}^{i-1} \sigma_j S_{i-j} + = 0 \quad (1 \leq i \leq \nu, i = even)$$

$$S_i + \sum_{j=1}^{\nu} \sigma_j S_{i-j} = 0 \quad (i \geq \nu) \tag{5}$$

Next, in order to simplify the decoding process, another set of identities related to S_{-i} and σ_j given in the following

$$S_{-i} + \sum_{j=1}^{i-1} \frac{\sigma_{\nu-j}}{\sigma_\nu} S_{-(i-j)} + \frac{\sigma_{\nu-i}}{\sigma_\nu} = 0 \quad (1 \leq i \leq \nu, i = odd)$$

$$S_{-i} + \sum_{j=1}^{i-1} \frac{\sigma_{\nu-j}}{\sigma_\nu} S_{-(i-j)} = 0 \quad (1 \leq i \leq \nu, i = even)$$

$$S_{-i} + \sum_{j=1}^{\nu} \frac{\sigma_{\nu-j}}{\sigma_\nu} S_{-(i-j)} = 0 \quad (i \geq \nu) \tag{6}$$

It is clear that for a t-error-correcting QR code that if there are $\nu \leq t$ errors in the received codeword, one must have $\sigma_{\nu+1} = \sigma_{\nu+2} = \sigma_t = 0$, and $S_0 \equiv \nu \bmod 2$.

If there is a sufficient number of consecutive known syndromes for a given number of errors, one can directly solve from the Newtons identities for the σ_j, $1 \leq j \leq \nu$. However, if there are not enough consecutive syndromes, one first tries to find the unknown syndromes and then to find $L(z)$ from the Newton identities. In either case, once $L(z)$ is found, the error pattern is found by a search of the roots of $L(z)$ over the set of all the nth roots of unity.

If not, assume that ν errors occur in the received vector. Let $I = \{i_1, i_2, \ldots, i_{\nu+1}\}$ and $J = \{j_1, j_2, \ldots, j_{\nu+1}\}$ denote two subsets of $\{1, 2, \ldots, n-1\}$. The matrices $X(I)$ and $X(J)$ are defined to have the following forms:

$$X(I) = \begin{pmatrix} Z_1^{i_1} & Z_2^{i_1} & \ldots & Z_\nu^{i_1} \\ Z_1^{i_2} & Z_2^{i_2} & \ldots & Z_\nu^{i_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{i_\nu} & Z_2^{i_\nu} & \ldots & Z_\nu^{i_\nu} \\ Z_1^{i_{\nu+1}} & Z_1^{i_{\nu+1}} & \ldots & Z_\nu^{i_{\nu+1}} \end{pmatrix}$$

and

$$X(J) = \begin{pmatrix} Z_1^{j_1} & Z_2^{j_1} & \ldots & Z_\nu^{j_1} \\ Z_1^{j_2} & Z_2^{j_2} & \ldots & Z_\nu^{j_2} \\ \vdots & \vdots & \ddots & \vdots \\ Z_1^{j_\nu} & Z_2^{j_\nu} & \ldots & Z_\nu^{j_\nu} \\ Z_1^{j_{\nu+1}} & Z_1^{j_{\nu+2}} & \ldots & Z_\nu^{j_{\nu+1}} \end{pmatrix} \tag{7}$$

See [1, 3]. Next, consider the matrix $S(I, J)$ of size $(\nu + 1) \times (\nu + 1)$ as follows:

$$S(I, J) = X(I)X(J)^T \tag{8}$$

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

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

where the summation of the subindices of the S_i's is modulo n , and $det(S(I, J)) = 0$. 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 detailed procedures to determine the primary unknown syndromes.

For an arbitrary binary QR code the following theorem, proved in Reference[1], holds.

Theorem 3.1. *[7] Let (n, k, d) be a binary QR code with Q, the set of quadratic residues modulo n, and the base set S. Then the error pattern has a weight of at most one if and only if the following two conditions hold:*

(i) $S_i = S_1^i \quad$ *for all* $i \in S$

(ii) $S_1^{n+1} = S_1$

A necessary and sufficient condition for exactly two errors to occur in the received codeword for the subclass of the QR codes of length $n = 8l + 1$ is found in the next theorem.

Theorem 3.2. *[7] Let* (n, k, d) *be a binary QR code of length* $n = 8l + 1$ *and quadratic residue set Q. Then, the error pattern has a weight of two if and only if the following conditions are satisfied:*

(i) $Tr(\frac{1}{S_1 S_{-1}}) = 0$ *where* $Tr(.)$ *denote the trace*

(ii) $S_i = Z_1^i + Z_2^i, \forall\ i \in S$ *where* Z_1 *and* Z_2 *are the roots of the quadratic equation,* $z^2 + S_1 z + \frac{S_1}{S_{-1}} = 0$

4 New algebraic decoding of the (41, 21, 9) QR code

The base set of the (41, 21, 9) QR code is $S = \{1\}$, a singleton set. Every known syndromes (respectively, unknown syndromes) can be expressed as some power of S_1 (resp.,S_3) as follows $S_2 = S_1^2$, $S_4 = S_1^4$, $S_5 = S_1^{128}$, $S_8 = S_1^8$, $S_9 = S_1^{32768}$, $S_{10} = S_1^{256}$, $S_{16} = S_1^{16}$, $S_{20} = S_1^{512}$, $S_{21} = S_1^{524288}$, $S_{23} = S_1^{64}$, $s_{25} = S_1^{16384}$, $S_{31} = S_1^{262144}$, $S_{32} = S_1^{32}$, $s_{33} = S_1^{8192}$, $S_{36} = S_1^{131072}$, $S_{37} = S_1^{4096}$, $S_{39} = S_1^{2048}$, $S_{-1} = S_{40} = S_1^{1024}$ and $S_{38} = S_3^{1024}$ see[8]. Since $t = \frac{(d-1)}{2} = 4$, this code allows for the correction of up to four errors. In other words, there are five cases to be considered :

Case 0: No error in the received codeword if and only if $S_1 = 0$; otherwise go to Case 1.

Case 1: One error in the received codeword if and only if the two conditions in Theorem 3.1 holds, i.e. $S_1^{41} = 1$; otherwise go to Case 2.

Case 2: Two errors in the received codeword if and only if the two conditions in Theorem 3.2 holds. From Theorem 3.1 and Theorem 3.2 one has

$$S_1 + \sigma_1 = 0 \tag{10}$$

$$S_{-1} + \frac{\sigma_1}{\sigma_2} = 0 \tag{11}$$

which, when solved, yields

$$\sigma_1 = S_1$$

$$\sigma_2 = \frac{S_1}{S_{-1}} = \frac{S_1}{S_{40}}$$

The error-locator polynomial is obtained from these $\sigma_k s$ as follows $L_2(z) = z^2 + \sigma_1 z + \sigma_2 = 0$, if $L_2(z)$ has the roots Z_1 and Z_2 with $Z_i^{41} = 1$ (i=1, 2), then two errors have occurred ; otherwise go to Case 3.

Case 3: For three errors, one has

$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + \sigma_3 = 0 \tag{12}$$

$$S_{-1} + \frac{\sigma_2}{\sigma_3} = 0 \tag{13}$$

$$S_{-3} + \frac{\sigma_2}{\sigma_3} S_{-2} + \frac{\sigma_1}{\sigma_2} S_{-1} + \frac{1}{\sigma_3} = 0 \tag{14}$$

The coefficients of the error-locator polynomial, found by solving equations 10, 12 and 13 are

$$\begin{aligned} \sigma_1 &= S_1 \\ \sigma_2 &= \frac{S_{-1}(S_3 + S_1^3)}{S_1 S_{-1} + 1} \\ \sigma_3 &= \frac{S_3 + S_1^3}{S_1 S_{-1} + 1} \end{aligned} \tag{15}$$

In this case the unknown syndrome S_3 can be determined by choosing $I_3 = \{0, 31, 39, 40\}$ and $J_3 = \{0, 1, 2, 5\}$, yields the matrix $S(I_3, J_3)$ of size 4×4 as follows

$$\begin{bmatrix} S_0 & S_1 & S_2 & S_5 \\ S_{31} & S_{32} & S_{33} & S_{36} \\ S_{39} & S_{40} & S_0 & S_3 \\ S_{40} & S_0 & S_1 & S_4 \end{bmatrix} = \begin{bmatrix} 1 & S_1 & S_1^2 & S_1^{128} \\ S_1^{262144} & S_1^{32} & S_1^{8192} & S_1^{131072} \\ S_1^{2048} & S_1^{1024} & 1 & S_3 \\ S_1^{1024} & 1 & S_1 & S_1^4 \end{bmatrix}$$

See [8], which satisfy $det(S(I_3, J_3)) = 0$. When solved, yields

$S_3 = S_1^3[S_1^{133086} + S_1^{250} + S_1^{373} + S_1^{263261} + S_1^{1148} + S_1^{9184} + S_1^{8409} + S_1^{8532} + S_1^{262113} + S_1^{10332} + S_1^{131036} + S_1^{262236} + S_1^{263138} + 1]/(S_1^{9184} + S_1^{8159} + S_1^{1025} + 1)$.

Next, it is necessary to find the condition for the case of exactly three errors with the known $\sigma_i (i = 1, 2, 3)$ in equation 15 . Given

$$S_1^2 S_{-1}^2 + 1 = (S_{-3} + S_{-1}^3)(S_3 + S_1^3) \tag{16}$$

If the conditions for case 0, case 1 and case 2 do not hold, equation 16 is also a sufficient condition for the case of exactly three errors.

Case 4: For four errors, one has

$$S_{-1} + \frac{\sigma_3}{\sigma_4} = 0 \tag{17}$$

$$S_{-3} + \frac{\sigma_3}{\sigma_4} S_{-2} + \frac{\sigma_2}{\sigma_4} S_{-1} + \frac{\sigma_1}{\sigma_4} = 0 \tag{18}$$

and

$$S_{-5} + \frac{\sigma_3}{\sigma_5} S_{-3} + \frac{\sigma_2}{\sigma_5} S_{-2} + \frac{\sigma_1}{\sigma_5} S_{-1} = 0 \tag{19}$$

which, when solved, yields

$$\begin{aligned}
\sigma_1 &= S_1 \\
\sigma_2 &= \frac{S_3 S_{38} + S_3 S_{39} S_{40} + S_1^3 S_{38} + S_1^3 S_{39} S_{40} + S_{40} S_1}{S_{38} S_1 + S_{39} S_{40} S_1 + S_{40}^2} \\
\sigma_3 &= \frac{S_{40}(S_{40} S_3 + S_{40} S_1^3 + S_1^2)}{S_{38} S_1 + S_{39} S_{40} S_1 + S_{40}^2} \\
\sigma_4 &= \frac{S_{40} S_3 + S_{40} S_1^3 + S_1^2}{S_{38} S_1 + S_{39} S_{40} S_1 + S_{40}^2}
\end{aligned} \tag{20}$$

Here, let $I_4 = \{0, 2, 8, 9, 20\}$ and $J_4 = \{0, 1, 23, 31, 37\}$, to have the matrix $S(I_4, J_4)$ of size 5×5 as follows

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

$$\begin{bmatrix} 0 & S_1 & S_1^{64} & S_1^{262144} & S_1^{4096} \\ S_1^2 & S_3 & S_1^{16384} & S_1^{8192} & S_1^{2048} \\ S_1^8 & S_1^{32768} & S_1^{262144} & S_1^{2048} & S_1^4 \\ S_1^{32768} & S_1^{256} & S_1^{32} & S_1^{1024} & S_1^{128} \\ S_1^{512} & S_1^{524288} & S_1^2 & S_1^{256} & S_1^{16} \end{bmatrix}.$$

determine S_3 by solving $det(S(I_4, J_4)) = 0$, to have
$S_3 = (1 + S_1^{2050} + S_1^{287} + S_1^{738} + S_1^{1804} + S_1^{1886} + S_1^{2091} + S_1^{2337} + S_1^{2788} + S_1^{4346} + S_1^{4633} + S_1^{6109} + S_1^{7954} + S_1^{8036} + S_1^{8241} + S_1^{8446} + S_1^{8733} + S_1^{12259} + S_1^{16482} + S_1^{17138} + S_1^{17630} + S_1^{18778} + S_1^{20705} + S_1^{23001} +$

$S_1^{32923} + S_1^{33579} + S_1^{36121} + S_1^{36572} + S_1^{36859} + S_1^{37597} + S_1^{40672} + S_1^{41369} + S_1^{45305} + S_1^{49118} + S_1^{50922} + S_1^{54489} + S_1^{67609} + S_1^{73513} + S_1^{77531} + S_1^{85977} + S_1^{262133} + S_1^{262236} + S_1^{262892} + S_1^{264163} + S_1^{265434} + S_1^{266459} + S_1^{270682} + S_1^{274905} + S_1^{278513} + S_1^{279005} + S_1^{294667} + S_1^{294749} + S_1^{296922} + S_1^{297209} + S_1^{302826} + S_1^{311641} + S_1^{329435} + S_1^{343785} + S_1^{524267} + S_1^{525087} + S_1^{526235} + S_1^{526809} + S_1^{527137} + S_1^{530171} + S_1^{532385} + S_1^{536321} + S_1^{545505} + S_1^{560921} + S_1^{565021} + S_1^{579289} + S_1^{786175} + S_1^{788225} + S_1^{791259} + S_1^{802657} + S_1^{831193} + S_1^{835293} + S_1^{1048411} + S_1^{1083097})/S_1^{161}(1 + S_1^{656} + S_1^{1148} + S_1^{2296} + S_1^{3936} + S_1^{4674} + S_1^{6236} + S_1^{32636} + S_1^{34440} + S_1^{38458} + S_1^{261744} + S_1^{261826} + S_1^{262236} + S_1^{267320} + S_1^{294462} + S_1^{298808} + S_1^{524472} + S_1^{556616})$

Next, it is necessary to find the condition for the case of exactly four errors with the known σ_i (i = 1, 2, 3, 4) in equation 19. Gives

$$[(S_3 + S_1^3)(S_{37}S_{40} + S_{38}S_{40}^2) + S_3S_{39}(S_{38} + S_{39}S_{40}) + S_1^3S_{39}(1 + S_{39}S_{40}) + S_1S_{39}S_{40}(1 + S_1S_{40}) + S_1(S_{40}^2 + S_1S_{37})]/[S_{40}(S_3 + S_1^3) + S_1^2] = 0 \quad (21)$$

A full computer search shows that, in the case of exactly four errors, $S_{40}(S_3 + S_1^3) + S_1^2$ is always nonzero. If the conditions for case 0, case 1, case 2 and case 3 do not hold, equation 21 is also a sufficient condition for the case of exactly four errors.
The flowchart of the entire process for decoding this code up to four errors is depicted in the flow diagram in Figure 1

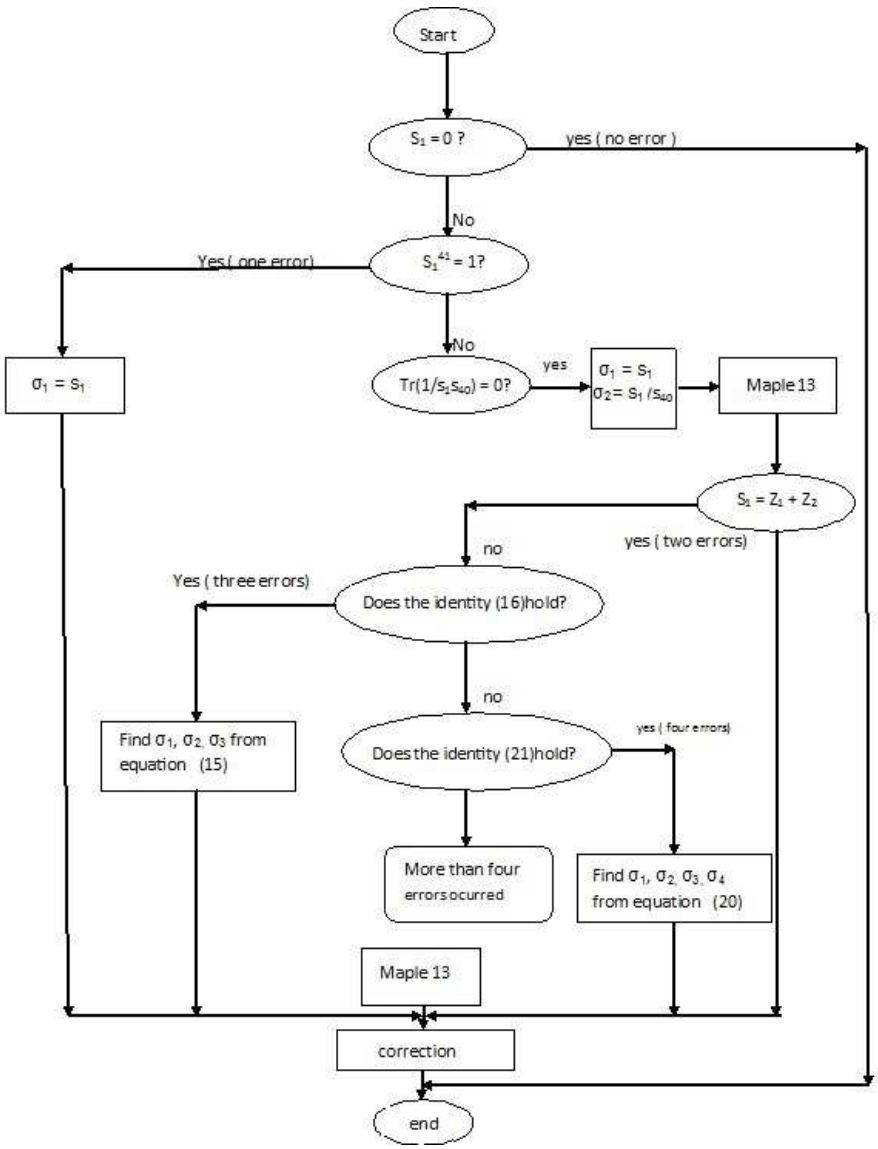

Figure 1: Flowchart of the algorithm for decoding the (41,21, 9) QR code

5 Conclusions

The finite field to implement the (41, 21, 9) QR code is $GF(2^{20})$. It contain 2^{20} elements. To calculate the syndrome polynomials over this field we use Maple 13. The algebraic method obtained in Section 4 for decoding the (41, 21, 9) QR code is able to correct all of the four errors and a sufficient condition for the case of ν errors is found for this code. It is expected that some of the techniques developed here can be used to simplify the decoding of other QR codes.

References

[1] Chang Y., Cheng H. Y.,Lee C. D., Reed I. S. and Truong T. K. : *Algebraic Decoding of* $(71, 36, 11)$*,* $(79, 40, 15)$*, and* $(97, 49, 15)$ *Quadratic Residue Codes*, IEEE Trans. Commun., vol.51, no.9, 2003, pp.1463-1473 .

[2] Chang Y., Cheng H. Y.,Lee C. D., Reed I. S. and Truong T. K. : *Algebraic Decoding of* $(103, 52, 19)$ *and* $(113, 57, 15)$ *Quadratic Residue Codes*, IEEE Trans. Inf. Theory, vol.53, no.5, 2005, pp.749 - 754.

[3] Chen Y. H., Chien C. H., Reed I. S. and Tai S. H., *Efficient Decoding of Systematic* $(41, 21, 9)$ *Quadratic Residue Code*, IEEE Asia-Pacific Services Computing Conference, 2008, pp. 128-133.

[4] Chang Y. and Lee C. D., *Decoding the* $(41, 21, 9)$ *Quadratic Residue Code* , IMECS, vol.2, 2010, pp.780-783 .

[5] Chen X., He R., Reed I. S. and Truong T. K. : *Decoding the* $(47, 24, 11)$ *Quadratic Residue Code*, IEEE Trans. Inf. Theory, vol.47 , no.3, 2001, pp.1181 -1186.

[6] Chen X., Reed I. S., Truong T. K. and Yin X. : *The Algebraic Decoding of the* $(41, 21, 9)$ *Quadratic Residue Code*, IEEE Trans. Inf. Theory, vol. 38, Issue 3,1992, pp. 974-986.

[7] Chen X., Reed I. S. and Truong T. K. : *Decoding the* $(73, 37, 13)$ *Quadratic Residue Code*, IEE Proc. Comput. Digit. Tech. , vol.141, no.5, 1994, pp.253 - 258 .

[8] Lin T. C, Shih P. Y., Su W. K. and Truong T. K. : *Decoding of the* $(41, 21, 9)$ *Quadratic Residue Code using the Gaos Algorithm*, IMECS, vol.2, 2008, pp.1209 - 1211.

[9] Prange E. : *Some Cyclic Error-Correcting Codes with Simple Decoding Algorithms*, Air Force Cambridge Research Center-TN-58-156, Cambridge, MA: 1958.