Decoding of the (41, 21, 9) Quadratic Residue Code Using the Gao's Algorithm

Wen-Ku Su, Pei-Yu Shih, Tsung-Ching Lin, and Trieu-Kien Truong

***Abstract*—In this paper, a decoding method is proposed for the (41, 21, 9) quadratic residue code. The method is acquired through applying the condition of the modified Gao's algorithm that is similar to fast transform decoding developed by Shiozaki [8]. The property of the syndrome polynomial is used in our decoding method. The new algorithm for has been verified by a software simulation using C^{++} language running through all error patterns.**

***Index Terms*—Quadratic residue codes, Gao' algorithm, unknown syndrome, error-locator polynomial, decoding algorithm.**

I. Introduction

The class of quadratic residue (QR) codes was introduced by Prange in 1958 [1]. It is a nice family of cyclic codes and has approximately 1/2 code rates. Most of the binary QR codes are the best known codes, such as Hamming code [2] and Golay code [3, 4].

The QR code with code length 41has the 4-error capacity since its minimum distance is nine. The procedure used most often to decoding the binary (41, 21, 9) QR code is the algebra decoding developed by Reed [5]. This scheme was used to solve the Newton identities that are non-linear, multivariate equations of quite high degree.

In this paper, to have the unknown syndrome S_3 is a necessary condition for decoding the (41, 21, 9) QR code. In 2001, a new technique to express the unknown syndromes as functions of known syndromes was developed by He *et al* [6]. We use the technique to determine the unknown syndrome S_3. Then the syndrome polynomial is obtained. Further, the determined syndrome polynomial is applied in the key equation of the Gao's algorithm given in [7-9]. The Gao's algorithm proposes an efficient condition that is suitable for the (41, 21, 9) QR code. Then we solve the key equation using the extended Euclidean algorithm (EEA) to obtain the error-locator polynomial. After Chain search, the error locations are confirmed.

This paper is organized as follows: Section 2 describes the (41, 21, 9) QR code. Our decoding algorithm of the (41, 21, 9) QR code and an example are offered in section 3. Finally, this paper concludes with a brief summary in section 4.

II. The (41, 21, 9) QR code

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, called Q_{41}, is equal to {1, 2, 4, 5, 8, 9, 10, 16, 18, 20, 21, 23, 25, 31, 32, 33, 36, 37, 39, 40}. The generator polynomial of binary (41, 21, 9) QR code can be written as

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

The received word $r(x)$ is represented as a polynomial is $r(x)=c(x)+e(x)=\sum_{i=0}^{40}c_i x^i+\sum_{i=0}^{40}e_i x^i$ where the codeword $c(x)$ equal to a message polynomial $m(x)$ multiply $g(x)$, $e(x)$ is the error polynomial and c_i , e_i belong to $GF(2)$.

The error locator polynomial is defined by

$$W(x)=\prod_{i=1}^{v}(1-X_i x) \quad (1)$$

Where v is the number of occurred errors, and X_i is the error location.

The syndrome is defined as $s_i=r(\beta^i)=c(\beta^i)+e(\beta^i)$ where $0\le i\le 40$. The relations among syndromes for the (41, 21, 9) QR code is given in following:

$S_2=S_1^2, S_4=S_1^4, S_8=S_1^8, S_{16}=S_1^{16}, S_{32}=S_1^{32},$

$S_{23}=S_1^{64}, S_5=S_1^{128}, S_{10}=S_1^{256}, S_{20}=S_1^{512}, S_{40}=S_1^{1024},$

$S_{39}=S_1^{2048}, S_{37}=S_1^{4096}, S_{33}=S_1^{8192}, S_{25}=S_1^{16384}, S_9=S_1^{32768},$

$S_{18}=S_1^{65536}, S_{36}=S_1^{131072}, S_{31}=S_1^{262144}, S_{21}=S_1^{524288}.$

$S_6=S_3^2, S_{12}=S_3^4, S_{24}=S_3^8, S_7=S_3^{16}, S_{14}=S_3^{32},$

$S_{28}=S_3^{64}, S_{15}=S_3^{128}, S_{30}=S_3^{256}, S_{19}=S_3^{512}, S_{38}=S_3^{1024},$

$S_{35}=S_3^{2048}, S_{29}=S_3^{4096}, S_{17}=S_3^{8192}, S_{34}=S_3^{16384}, S_{27}=S_3^{32768},$

$S_{13}=S_3^{65536}, S_{26}=S_3^{131072}, S_{11}=S_3^{262144}, S_{22}=S_3^{524288}.$

If i belong to Q_{41}, the syndromes are called the known syndromes and have the property

$$s_i=r(\beta^i)=e(\beta^i) \text{ for } i\in Q_{41} \quad (2)$$

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

For the binary (41, 21, 9) QR code, every known syndromes (resp., unknown syndromes) can be expressed as

Manuscript received Jannuary 8, 2008. The work was supported by National Science Council, R.O.C., under Grants NSC95-2221-E-214-042.

Wen-Ku Su is with the Department of Information Engineering, I-Shou University, Tahsu, 84001, Kaohshiung, Taiwan (886-939913808; fax: 886-7-6577293; e-mail: d9403003@stmail.isu.edu.tw).

Pei-Yu Shih is with the Department of Information Engineering, I-Shou University, Tahsu, 84001, Kaohshiung, Taiwan (e-mail: d9203005@stmail.isu.edu.tw).

Tsung-Ching Lin is with the Department of Information Engineering, I-Shou University, Tahsu, 84001, Kaohshiung, Taiwan (e-mail: joe@isu.edu.tw).

Trieu-Kien Truong is with the Department of Information Engineering, I-Shou University, Tahsu, 84001, Kaohshiung, Taiwan (e-mail: truong@isu.edu.tw).

some power of S_1 (resp.,S_3). For the detail about syndromes, we refer the reader to [10].

III. New Decoding Algorithm of the (41, 21, 9) QR Code

Recall the EEA when applied to find the greatest common divisor (g.c.d) of two nonzero polynomials *a*, and *b* over *GF*(*q*). If we use the EEA to determine the g.c.d of *T*(*x*) and x^{41}-1, we generate sets of solutions $(W^{(l)}(x), P^{(l)}(x), \theta^{(l)}(x))$. $W^{(l)}(x)$ and $P^{(l)}(x)$ are useful for our decoding method. The condition of the Gao's algorithm, $\deg P^{(l)}(x) \le (n+k)/2$, is suitable for the (41, 21, 9) QR code. The particular solution $W^{(l)}(x)$ is the error locator polynomial when $P^{(l)}(x)$ has degree less than 62/2. Let polynomial *S*(*x*) (resp., 1+*S*(*x*)) replaces to *T*(*x*), when the weight *v* of *E*(*x*) is odd (resp., even). Consequentially, the new decoding algorithm for the (41, 21, 9) QR code and an example are given in the following.

If the received polynomial *r*(*x*) is zero, there is no error in the received word. When the errors occur in received word, the decoding algorithm is summarized below by nine steps.

- Step 1. Evaluate the known syndromes by using Eq. (2)
- Step 2. Initialize by letting *v*=1.
- Step 3. Compute the unknown syndromes by applying the technique in [10].
- Step 4. Applying the EEA to x^{41}-1 and *T*(*x*) to determine the polynomial $W^{(l)}(x)$.
- Step 5. Applying Chien search to find the roots of $W^{(l)}(x)$.
- Step 6. If there are exists *v* errors, go to Step8. Otherwise, set *v*=*v*+1.
- Step 7. If *v*>4, stop. If not, go to Step3.
- Step 8. The error polynomial is determined and then the received word can be corrected.

Example_Decoding the (41, 21, 9) *QR code using the new algorithm*

We consider the information polynomial $I(x)$ equal to $1+x^5+x^9+x^{10}+x^{14}+x^{15}+x^{16}+x^{19}+x^{20}$, then the code polynomial *c*(*x*) is

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

which is a multiple of *g*(*x*). We assume that the error polynomial *e*(*x*) is $1+x^2+x^{10}+x^{30}$.

Then the received polynomial is the sum of the code polynomial *c*(*x*) and the error polynomial *e*(*x*), i.e. *r*(*x*)=

$$c(x)+e(x) = x^3+x^7+x^8+x^9+x^{10}+x^{15}+x^{16}+x^{19} + x^{22}+x^{24}+x^{26}+x^{28}+x^{29}+x^{31}+x^{33} + x^{34}+x^{35}+x^{36}+x^{37}+x^{38}+x^{40},$$

The decoding process developed in this paper is described as follows. First of all, the known syndrome S_i for each *i* in Q_{41} can be calculated from the received polynomial *r*(*x*) in Eq. (2).

By evaluating *r*(*x*) at the roots of *g*(*x*) mentioned above, the primary known syndrome is $S_1 = \alpha^{22533} \neq 0$, 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 $S_3 = S_1^3 = \alpha^{67599}$. After the determination of the primary syndromes S_1 and S_3, all syndromes can be also determined. Therefore, we further obtain the syndrome polynomial.

The EEA is applied to polynomial *T*(*x*)=*S*(*x*) and x^{41}-1. One observes that $\deg(P_i(x)) = 17 < (41+21)/2 = 31$. Thus, the error locator polynomial *W*(*x*) with degree 30 is obtained as follows:

$$\alpha^{143897}x+\alpha^{166430}x^2+\alpha^{283025}x^3+\alpha^{305558}x^4+\alpha^{316616}x^5+\alpha^{425836}x^6 + \alpha^{765354}x^7+\alpha^{320914}x^8+\alpha^{1019594}x^9+\alpha^{899537}x^{10}+\alpha^{285342}x^{11} + \alpha^{524612}x^{12}+\alpha^{755466}x^{13}+\alpha^{720597}x^{14}+\alpha^{217804}x^{15}+\alpha^{1025111}x^{16} + \alpha^{135916}x^{17}+\alpha^{966197}x^{18}+\alpha^{877024}x^{19}+\alpha^{627566}x^{20}+\alpha^{596236}x^{21} + \alpha^{477997}x^{22}+\alpha^{848555}x^{23}+\alpha^{802996}x^{24}+\alpha^{593558}x^{25}+\alpha^{273784}x^{26} + \alpha^{29410}x^{27}+\alpha^{24268}x^{28}+\alpha^{70124}x^{29}+\alpha^{64982}x^{30}$$

Using Chien search to find the root of the *W*(*x*), there are more than one root $\{\beta^i \mid 0 \le i \le 40\}$ in *W*(*x*), and thus the assumption is not valid.

If the number of the errors is two, the primary unknown syndrome S_3 can be determined by the technique developed in [10]. 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 [4], the determinant of the above matrix is zero. The unknown syndrome S_3 for the two-error case is thus

$$S_3 = \frac{S_1S_2S_9 + S_2^2S_8 + S_1^2S_{10}}{S_1S_8} = \alpha^{313583},$$

where S_0=0 and S_1= α^{22533}. Since *v*=2 is even, the polynomial *T*(*x*)=1+*S*(*x*) is used in the EEA. Similarly, the error locator polynomial is determined in the following:

$$1+\alpha^{22533}x+\alpha^{92619}x^2+\alpha^{92116}x^3+\alpha^{153763}x^4+\alpha^{668096}x^5 + \alpha^{735902}x^6+\alpha^{300293}x^7+\alpha^{962484}x^8+\alpha^{605771}x^9+\alpha^{654474}x^{10} + \alpha^{48190}x^{11}+\alpha^{479187}x^{12}+\alpha^{783458}x^{13}+\alpha^{736261}x^{14}+\alpha^{944274}x^{15} + \alpha^{132879}x^{16}+\alpha^{614478}x^{17}+\alpha^{910743}x^{18}+\alpha^{481441}x^{19}+\alpha^{17420}x^{20} + \alpha^{681167}x^{21}+\alpha^{415413}x^{22}+\alpha^{354587}x^{23}+\alpha^{502759}x^{24}+\alpha^{144252}x^{25} + \alpha^{244875}x^{26}+\alpha^{774272}x^{27}+\alpha^{987564}x^{28}+\alpha^{142778}x^{29}+\alpha^{137636}x^{30}$$

Using Chien search to find the root of the *W*(*x*), there are more than two roots $\{\beta^i \mid 0 \le i \le 40\}$ in *W*(*x*), and thus the assumption is not valid.

If the number of the errors is three, the primary unknown syndrome S_3 can be determined [10] by the following:

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

where S_0=1 and $S_1 = \alpha^{22533}$. Since *v*=3 is odd, the polynomial *T*(*x*)=*S*(*x*) is used in the EEA. Similarly, the error

locator polynomial is determined in the following:

$$\alpha^{878231}x+\alpha^{900764}x^2+\alpha^{834719}x^3+\alpha^{1017658}x^4+\alpha^{736286}x^5$$
$$+\alpha^{515814}x^6+\alpha^{813172}x^7+\alpha^{861630}x^8+\alpha^{385883}x^9+\alpha^{392513}x^{10}$$
$$+\alpha^{580001}x^{11}+\alpha^{594792}x^{12}+\alpha^{452250}x^{13}+\alpha^{960190}x^{14}+\alpha^{724163}x^{15}$$
$$+\alpha^{474835}x^{16}+\alpha^{764049}x^{17}+\alpha^{318385}x^{18}+\alpha^{445753}x^{19}+\alpha^{864115}x^{20}$$
$$+\alpha^{963403}x^{21}+\alpha^{574230}x^{22}+\alpha^{109016}x^{23}+\alpha^{367350}x^{24}+\alpha^{651013}x^{25}$$
$$+\alpha^{385432}x^{26}+\alpha^{868934}x^{27}+\alpha^{570939}x^{28}+\alpha^{149127}x^{29}+\alpha^{143985}x^{30}$$

A full computer search shows that there are more than three roots β^i for $0 \le i \le 40$ to satisfy $W(\beta^i)=0$, and therefore the assumption is not valid.

If the number of the errors is four, i.e., v=4, the primary unknown syndrome S_3 can be determined as follows:

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

where $S_0=0$ and $S_1=\alpha^{22533}$. The unknown syndrome S_3 for the four-error case is $S_3=\alpha^{1036507}$. Therefore, we further obtain the syndrome polynomial

$$S(x)=\alpha^{22533}x+\alpha^{45066}x^2+\alpha^{1036507}x^3+\alpha^{90132}x^4+\alpha^{787074}x^5$$
$$+\alpha^{1024439}x^6+\alpha^{855487}x^7+\alpha^{180264}x^8+\alpha^{164544}x^9$$
$$+\alpha^{525573}x^{10}+\alpha^{1045558}x^{11}+\alpha^{1000303}x^{12}+\alpha^{785677}x^{13}$$
$$+\alpha^{662399}x^{14}+\alpha^{552446}x^{15}+\alpha^{360528}x^{16}+\alpha^{753569}x^{17}$$
$$+\alpha^{329088}x^{18}+\alpha^{112634}x^{19}+\alpha^{2571}x^{20}+\alpha^{535554}x^{21}$$
$$+\alpha^{1042541}x^{22}+\alpha^{393537}x^{23}+\alpha^{952031}x^{24}+\alpha^{82272}x^{25}$$
$$+\alpha^{522779}x^{26}+\alpha^{917126}x^{27}+\alpha^{276223}x^{28}+\alpha^{901072}x^{29}$$
$$+\alpha^{56317}x^{30}+\alpha^{267777}x^{31}+\alpha^{721056}x^{32}+\alpha^{41136}x^{33}$$
$$+\alpha^{458563}x^{34}+\alpha^{450536}x^{35}+\alpha^{658176}x^{36}+\alpha^{20568}x^{37}$$
$$+\alpha^{225268}x^{38}+\alpha^{10284}x^{39}+\alpha^{5142}x^{40}$$

Since v=4 is even, the polynomial $T(x)$=1+$S(x)$ is used in EEA. Similarly, the error locator polynomial is determined as follows:

$$W(x)=1+\alpha^{22533}x+\alpha^{863025}x^2+\alpha^{30717}x^3+\alpha^{25575}x^4,$$

and there exists exactly four roots β^0, β^{-2}, β^{-10}, β^{-30} in $W(x)$ via Chien search. In other words, the error polynomial $e(x)=1+x^2+x^{10}+x^{30}$ is determined.

IV. Conclusion

In this paper, a new decoding algorithm of the (41, 21, 9) QR code is proposed. We apply the key equation of the Gao's algorithm in our decoding method. The key equation of the Gao's algorithm supplies a successful condition to determine the error locator polynomial. It would be interesting to see if there exists the condition to determine the number of occurred four-errors.

References

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

[2] R. W. Hamming, Error detecting and error correcting codes, *Bell System Technical Journal* 29 (2) (1950) 147-160.

[3] M. Elia, "Algebraic decoding of the (23, 12, 7) Golay code," *IEEE Trans. Inf. Theory*, vol. 33, pp. 150-151, Jan. 1987.

[4] Gregory O. Dubney and Irving S. Reed, "Decoding the (23, 12, 7) Golay Code Using Bit-Error Probability Estimates," *IEEE GLOBECOM*, pp. 1325-1330, 2005.

[5] I. S. Reed, T. K. Truong, X. Chen, and X. Yin, The algebraic decoding of the (41, 21, 9) quadratic residue code, *IEEE Trans. Inf. Theory* 38 (3) (1992) 974-985.

[6] R. He, I. S. Reed, T. K. Truong, and X. Chen, "Decoding the (47, 24, 11) quadratic residue code," *IEEE Trans. Inf. Theory*, vol. 47, pp. 1181-1186, Mar. 2001.

[7] S. Gao, "A new algorithm for decoding Reed-Solomon codes," in Communications, Information and Network Security, V. Bhargava, H. V. Poor, V. Tarokh, and S. Yoon, Eds. Norwell, MA: Kluwer, 2003, vol. 712, pp. 55-68.

[8] L. Welch and E. R. Berlekamp, "Error Correction for Algebraic Block Codes," US Patent 4 633 470, 1983.

[9] Sergei V. Fedorenko, "A Simple Algorithm for Decoding Reed-Solomon Codes and its Relation to the Welch-Berlekamp Algorithm," *IEEE Trans. Inf. Theory*, vol. 51, pp. 1196-1198, Mar. 2005.

[10] Y. Chang, T. K. Truong, I. S. Reed, H. Y. Cheng, and C. D. Lee, Algebraic decoding of (71, 36, 11), (79, 40, 15), and (97, 49, 15) quadratic residue codes, *IEEE Trans. Inform. Theory* 51 (9) (2003) 1463-1473.

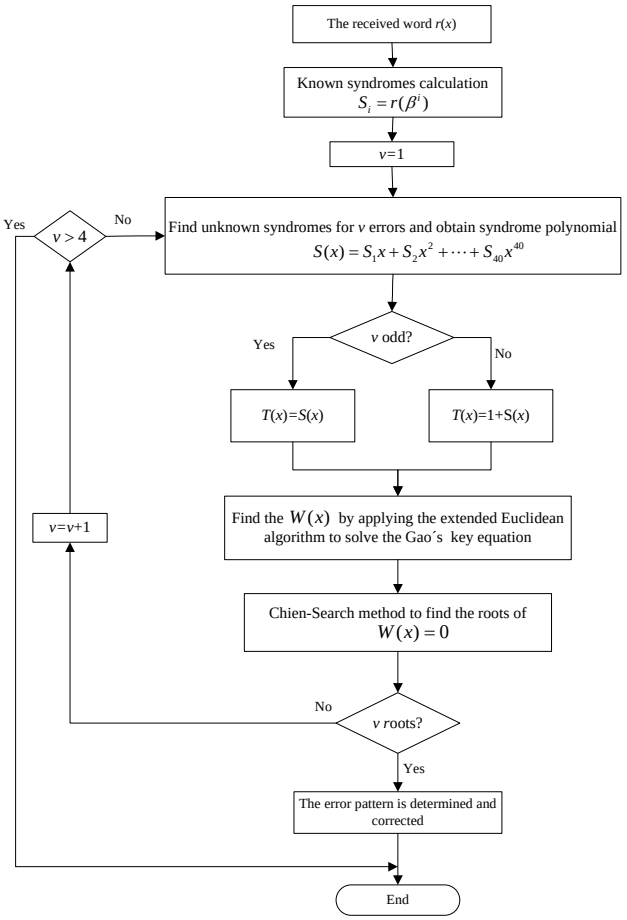

Fig. 1: Flowchart of the (41, 21, 9) QR decoder