

Channel Coding Report

-----Quadratic Residue Codes

Instructor: Professor C.H.Wei & Professor H.M.Hang

Students : 徐啓益(8911616) & 鍾瑞元(8911627)

Codes:

Definition of e-th Residue:

If n is a prime, and if e divides $n-1$, then i is a e -th residue if there exists an integer X such that $X^e = i \pmod n$

Definition of Quadratic Residue(QR):

An integer i is a quadratic residue of a prime n if there exists an integer X such that

$$X^2 = i \pmod n$$

Then we can define the set below:

Q: the set of quadratic residues, modulo a prime integer n .

$$Q = \{i^2 \pmod n \mid i \in \text{GF}(n), i \neq 0\} \text{ and the range of } i \text{ is } (1, [n-1/2])$$

$$\text{therefore } Q = \{i^2 \pmod n \mid i = 1, 2, \dots, \frac{n-1}{2}\}$$

e.g : Show each member of the Quadratic Residue Set for $n=17$

sol : Since $n=17 \rightarrow i = 1,2,3,\dots,8$

$$1^2 \bmod 17 = 1 \quad 2^2 \bmod 17 = 4$$

$$3^2 \bmod 17 = 9 \quad 4^2 \bmod 17 = 16$$

$$5^2 \bmod 17 = 8 \quad 6^2 \bmod 17 = 2$$

$$7^2 \bmod 17 = 15 \quad 8^2 \bmod 17 = 13$$

Therefore $Q=\{1,2,4,8,9,13,15,16\}$

Generating Polynomial:

Generating polynomial of Q: $q(x) = \prod_{r \in Q} (x + \alpha^r)$ (Augmented Form)

Generating polynomial of Q': $(x + 1)q(x)$ (Expurgated Form)

Where α is a primitive n -th root of unity in an the extension field of $GF(2)$.

e.g. $n=7 \rightarrow Q=\{1,2,4\}$ then for the $(7,4,3)$ QR code ,

the generating polynomial could be

$$q(x)=(x+1)(x^2+1)=x^3+x+1$$

Parameters of QR codes : length n and dimension k

Length n

Theorem : If n is a prime $= \pm 1 \pmod{8}$ then $2^{(n-1)/2} = 1 \pmod{n}$

According the theorem above, QR codes of length n over $GF(2)$

exist

iff $n = 8m \pm 1$

Dimension k :

The dimension of the QR code is $k = \begin{cases} \frac{1}{2}(n+1) & \text{for Q, N,} \\ \frac{1}{2}(n-1) & \text{for Q', N.'} \end{cases}$

Minimum Distance:

(i) Lower Bound

Theorem 1: Let d be the minimum Hamming Weight of the codewords which occur in augmented e -th residue code of length n over $GF(q)$ then $d^e > n$

Proof: see [1] p.158

Apply the theorem 1,

we can get the lower bound of QR codes : $d^2 > n$

(ii) Tighter Lower Bound

Theorem 2: If n is a prime $\equiv -1 \pmod{4}$, then the minimum Hamming Weight of the codewords in augmented QR code of length n is bounded by $d^2 - d + 1 > n$

(iii) another Lower Bound

Theorem 3: For the binary QR code of length n , the minimum weight d is bounded by $d^2 > n$ if $n \equiv +1 \pmod{8}$ (e.g $n=17$)
or $d(d-1) > n-1$ if $n \equiv -1 \pmod{8}$ (e.g $n=7$)

Minimum distance of certain augmented QR codes of length n over $GF(2)$

n	d
7	3
17	5
23	7
31	7
41	9
47	11
71	11
73	13
79	15
89	17
97	15
103	≤ 19
113	≤ 15
127	≤ 19
137	≤ 21

Decoding:

Let a codeword $c(x)=a(x)g(x)$ be transmitted through a noisy channel to obtain a received codeword of the form $r(x)=c(x)+e(x)$, where $e(x)$ is the polynomial of the received error pattern vector.

The syndromes: $s_i = e(\alpha^i) \quad i \geq 0$

$$s_i = 0 + e(\alpha^i) = c(\alpha^i) + e(\alpha^i) = r(\alpha^i) \quad i \in Q$$

in terms of symmetric polynomials

$$s_i = Z_1^i + Z_2^i + \dots + Z_v^i \quad i \geq 0 \quad s_i \in GF(2^q)$$

where Z_j for $1 \leq j \leq v$ are the locations of the v errors, i.e. $Z_j = \alpha^{r_j}$ with the

r_j being the locations of the errors and $v \leq t$ for $t=(d-1)/2$

Lemma 1:

(The existence and uniqueness of the solutions of the n nonlinear equations in the v unknown error locations and $(n-1)/2$ unknown syndromes.)

The mapping between the syndromes s_i of a QR code and the error pattern $e(x)$ of the weight $\leq t$ is one-to-one.

The aim of decoding is to find the v unknown errors locations from the known syndromes s_i for $i \in Q$.

The *error-locator polynomial* $L(z)$ for every correctable error pattern

$$L(z) = \prod_{i=1}^v (z - Z_i) = z^v + \sum_{j=1}^v \sigma_j z^{v-j}$$

the set $\{\sigma_i\}$, the coefficients of the $L(z)$, are related by

elementary symmetric functions of the error locations Z_i for $i = 1, 2, \dots, v$

$$\sigma_i = \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq v} Z_{j_1} Z_{j_2} \dots Z_{j_i} \quad (1 \leq i \leq v)$$

Algebraic Decoding Method

The **algebraic decoding method** consists primarily of the two steps.

- (1) the syndromes s_i for $i \in Q$ are used to determine the coefficients σ_j of $L(z)$.
- (2) the error pattern of the received code is be found by a Chien search of $L(z)$.

e.g : Decoding QR(47,24,11) codes by using algebraic decoding method, only up to 3 errors detection is considered here.

Sol:

For QR code (47,24,11),

$$Q = \{1, 2, 3, 4, 6, 7, 8, 9, 12, 14, 16, 17, 18, 21, 24, 25, 27, 28, 32, 34, 36, 37, 42\}$$

*Case 0: No error in the received codeword iff $S_1=0$,
otherwise go to Case 1.*

*Case 1: One error in the received codeword iff $S_1^{47}=1$
otherwise go to Case 2.*

Case 2: For receiving 2 errors in codeword, we have

$$S_1 + \sigma_1 = 0$$

$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 = 0$$

$$\text{And we also know that } S_2 = S_1^2$$

$$\text{Solve the equations } \rightarrow (\sigma_1, \sigma_2) = (S_1, S_1^{-1} S_3 + S_2)$$

Then the error locator polynomial is obtained.

$$L_2(z) = z^2 + S_1 z + S_1^{-1} S_3 + S_2$$

Solving $L_2(z) = 0 \rightarrow$ we get the roots z_1 & z_2

If $z_1 = z_2 = 1$, then 2 errors occur.

Otherwise go to Case 3.

Case3: for 3 errors, we have

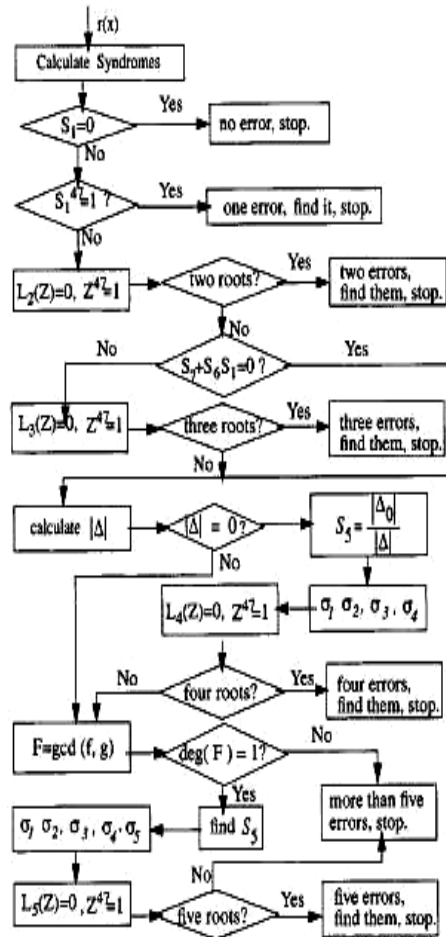
$$S_1 + \sigma_1 = 0$$

$$S_3 + \sigma_1 S_2 + \sigma_2 S_1 + \sigma_3 = 0$$

$$S_9 + \sigma_1 S_8 + \sigma_2 S_7 + \sigma_3 S_6 = 0$$

Similarly, Solve $(\sigma_1, \sigma_2, \sigma_3)$, we can get the $L_3(z)$

Solving $L_3(z) = 0$, we can determine whether there are 3 errors or not.



Flow Chart for decoding QR(47,24,11) up to 5 errors

Ref

- [1] Berlekamp, “Algebraic Coding Theory” ,1968
- [2] Ian F.Blake and Ronald C.Mullin,
”The Mathematical Theory of Coding”,1975
- [3] X.Chen and I.S.Reed,
“Error-Control Coding for Data Network”,1999
- [4] X. Chen and I. S. Reed,
”A Performance Comparison of the Binary Quadratic
Residues Codes with the 1/2-Rate Convolution Codes,”
IEEE Trans. Inform. Theory, vol.40, no.1, pp.126-136, Jan.
1994.
- [5] X. Chen, I. S. Reed, and T. K. Truong,
”A Performance Comparison of the Binary Quadratic
Residues Codes with the 1/2-Rate Convolution Codes,”
IEEE Proc.-Comput. Digit. Tech., vol.141, no.5,
pp.253-258, Sep. 1994.