Decoding the (41, 21, 9) Quadratic Residue Code

Chong-Dao Lee, Yaotsu Chang *

Abstract—**This paper proposes an algebraic decoding algorithm for the (41, 21, 9) quadratic residue code via Lagrange interpolation formula to determine error check and error locator polynomials. Programs written in C++ language have been executed to check every possible error pattern of this quadratic residue code.**

Keywords: Lagrange interpolation formula, quadratic residue code, error locator polynomial

1 Introduction

Quadratic residue codes [1] are a class of good algebraic error-correcting codes due to its large minimum distance. Recent research on quadratic residue codes is devoted to developing the algebraic decoding method [2]-[6], determining weight distribution [7], finding double circulant presentation [8], and improving the bounds of the minimum distance [9]. In particular, the algebraic decoding of the (41, 21, 9) binary quadratic residue codes [10] was based on the unknown syndrome [11]-[15], error locator polynomial [12]-[15], and lookup table [16].

In this paper, the Lagrange interpolation formula instead of the previous algebraic methods, such as syndrome matrix and Newton identities, is utilized to derive the error check and error locator polynomials for the use of decoding algorithm of the (41, 21, 9) quadratic residue code. Programs written in C++ language have been executed to check every possible error pattern of this quadratic residue code. Moreover, the decoding algorithm proposed here requires much less computational time than Algorithm D2 in [6].

Section 2 describes the brief introductions concerning QR code, syndrome, Lagrange interpolation formula. Section 3 defines the error check and error locator polynomials. Also, these polynomials are determined by Lagrange interpolation formula and are used in the proposed decoding algorithm in Section 4. Conclusions are given in the final section of the paper.

*Departments of Communication Engineering and Applied Mathematics, I-Shou University, Taiwan, R.O.C. Tel/Fax: 886-7-6577711/6578930 Email: {chongdao, ytchang}@isu.edu.tw

2 Preliminaries

2.1 Quadratic Residue Code

Let n be a prime number of the form $n \equiv \pm 1 \pmod 8$. A binary quadratic residue code of length n is an $(n, (n+1)/2, d)$ cyclic code with a generator polynomial $g(x) = \prod_{i \in Q}(x - \beta^i)$, where d stands for the minimum distance, the set $Q = \{i | i \equiv j^2 \bmod n \text{ for } 1 \le j \le n-1\}$ is the collection of all nonzero quadratic residues modulo n and β is a primitive nth root of unity in $\mathbb{E} = GF(2^m)$ satisfying $n \mid 2^m - 1$.

2.2 Syndrome

Let the code polynomial $c(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$ be transmitted through a noisy channel to obtain the received polynomial of the form $r(x) = c(x) + e(x)$, where $e(x) = e_0 + e_1 x + \cdots + e_{n-1}x^{n-1}$ is an error polynomial. The known syndromes are obtained by evaluating $r(x)$ at the roots of $g(x)$, i.e.,

$$S_i = r(\beta^i) = c(\beta^i) + e(\beta^i) = e(\beta^i), \quad i \in Q. \tag{1}$$

If $i \notin Q_n$, then define $S_i = e_0 + e_1(\beta^i) + \cdots + e_{n-1}(\beta^i)^{n-1}$ and call it *unknown syndrome*. When v errors occur in the received polynomial $r(x)$, then the error polynomial $e(x)$ has v nonzero terms, namely, $e(x) = x^{l_1} + x^{i_2} + \cdots + x^{l_v}$, where $0 \le l_1 < l_2 < \cdots < l_v \le n-1$. For a quadratic residue code with minimum distance d, an error polynomial $e(x)$ 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 $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. By definition, the syndrome S_i can be written as $S_i = (\beta^{l_1})^i + (\beta^{l_2})^i + \cdots + (\beta^{l_v})^i$, where β^{l_j} for $1 \le j \le v$ are called the *error locators*. For any binary cyclic codes, there is an obvious relation among syndromes, namely, $S_{2i} = S_i^2$, with sub-indices modulo n, if necessary.

2.3 Lagrange Interpolation Formula

The finite field version of Lagrange interpolation formula can be found in [17] and is as follows: for $q \ge 0$ let $a_0,\ a_1, \ldots,\ a_q$ be $q+1$ distinct elements of $\mathbb{E}$, and let $b_0,\ b_1, \ldots, b_q$ be $q+1$ arbitrary elements of $\mathbb{E}$. Then there exists exactly one polynomial $L(x) \in \mathbb{E}[x]$ of degree at most q such that $L(a_i) = b_i$ for $i = 0,\ 1, \ldots,\ q$. The

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

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 $h(x)$.

3 Key Polynomials

3.1 Error Check Polynomial

Let $\mathcal{E}^{(v,v+1)}$ be the set of all syndromes obtained from correctable error patterns of weights v and $v+1$.

Definition 1: The *error check polynomial* $H^{(v,v+1)}(x) = \prod_{\kappa \in \mathcal{E}^{(v,v+1)}}(x - \kappa)$ is a polynomial in x^n over $\mathbb{F}_2$.

For the (41, 21, 9) binary quadratic residue code, the error check polynomials are

$$\begin{aligned} H^{(1,2)}(x) &= 1 + x^{82} + x^{123} + x^{164} + x^{246} + x^{287} \\ &+ x^{328} + x^{369} + x^{492} + x^{533} + x^{574} \\ &+ x^{656} + x^{697} + x^{738} + x^{779} + x^{861} \end{aligned} \quad (2)$$

and

$$H^{(3,4)}(x) = \sum_{i \in Z} x^i. \quad (3)$$

To save space, instead of showing Z, we just show $\langle Z \rangle$ in (7), where $\langle \cdot \rangle$ is defined in the next subsection.

3.2 Error Locator Polynomial

For a binary quadratic residue code generated by irreducible polynomial, let $\sigma^{(v,v+1)}$ be an *error locator polynomial* in $\mathbb{F}_2[S_1, z]$ if

$$\sigma^{(v,v+1)}(S_1, z) = 1 + \sum_{j=1}^{v+1} \tilde{\sigma}_j(S_1) z^j, \quad (4)$$

where $1 \le j \le 4$, $\tilde{\sigma}_j \in \mathbb{F}_2[S_1]$ for a given correctable syndrome S_1 corresponding to an error pattern of weight v or $v+1$.

For the $(41, 21, 9)$ binary quadratic residue code, if $v = 1$, then

$$\sigma^{(1,2)}(S_1, z) = 1 + \tilde{\sigma}_1(S_1) z + \tilde{\sigma}_2(S_1) z^2, \quad (5)$$

where $\tilde{\sigma}_1(x) = x$ and $\tilde{\sigma}_2(x) = x^{166} + x^{248} + x^{289} + x^{330} + x^{371} + x^{535} + x^{617} + x^{658} + x^{699} + x^{822}$. If $v = 3$, then (4) becomes

$$\sigma^{(3,4)}(S_1, z) = 1 + \sum_{j=1}^{4} \tilde{\sigma}_j(S_1) z^j, \quad (6)$$

where $\tilde{\sigma}_1(x) = x$, $\tilde{\sigma}_2(x) = \sum_{i \in U_2} x^i$, $\tilde{\sigma}_3(x) = \sum_{j \in U_3} x^j$, and $\tilde{\sigma}_4(x) = \sum_{k \in U_4} x^k$. The hexadecimal sequences $\langle U_2 \rangle$, $\langle U_3 \rangle$, and $\langle U_4 \rangle$ are given in (8), (9), and (10), respectively.

Remark: for example, let $n = 41$ and $A = \{125, 207, 248, 289\}$. Since every number in the index set A is congruent to $r = 2$ modulo $n = 41$, to save space, subtract 2 and then divide by 41 for each number of A to obtain $\{3, 5, 6, 7\}$. Use numbers of this set to indicate the positions of 1 in a binary sequence, which yields the sequence 00010111. Convert it into a hexadecimal sequence, which is $8e$ in the case, and denote the final result by $\langle A \rangle$, i.e., $\langle A \rangle = 8e$.

Now we are ready to propose an algorithm for decoding the (41, 21, 9) binary quadratic residue code up to its error-correcting capacity as shown in the next section.

4 Decoding Algorithm

If the known syndromes calculated by (1) are all zeros, there is no error in the received word. The received word is really a codeword. When the errors occur in the received word, the decoding algorithm is described below by seven steps.

1. Compute the primary known syndrome S_1 from (1).
2. Initialize by letting $v = 1$.
3. Compute the error check polynomial $H^{(v,v+1)}(S_1)$ for in (2) or (3).
4. If $H^{(v,v+1)}(S_1) = 0$, go to step 6. Otherwise, set $v = v + 2$.
5. If $v > 4$, stop. Otherwise, go to step 3.
6. Compute the error locator polynomial $\sigma^{(v,v+1)}(S_1, z)$ in (5) or (6).
7. The error pattern is determined by the Chien search method and then the received word can be corrected.

5 Conclusions and Future Work

The Lagrange interpolation formula presented in this paper provides a practical technique to determine the error check and error locator polynomials. An interesting open problem remains whether there exists some simpler error-locator polynomials for the (41, 21, 9) binary quadratic residue code that is suitable for both software and hardware implementations.

Acknowledgment

The work was supported by National Science Council, R.O.C., under Grants NSC97-2221-E-214-027-MY2 and NSC97-2115-M-214-001-MY2.

References

[1] MacWilliams, F.J., Sloane, N.J.A., *The Theory of Error-Correcting Codes*, North-Holland, 1977.

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

$$\langle Z \rangle = d799f67dbc6e88632b7f7a4e4f6a44e7ae270109765fbf2bf584c746397a9306e8aff52a2d8b2ae1ef234761f 3faa148b407b9db2536b781440497595fa0a548d0436be07f16b2a1158645a5b280e35f1894bbfd5ce8e920a5a 7d425c6b3994b64c3e6a046ee1bb10dece7d4855cec202d2cdf4e549af8a323c7525512b19f52e3d8695626a73 d6f67c59f9fbfcf4121648edd089ae6af4090488fff5f7099c393bef1cdf1339193814880e86e50ba2c2e2acf41 11092d9bf0e59490341f94ec45913caa0516479c2638e1ed1df281c7800de77e134c82fb8542b0851e00d8c78f c790c1e92b5ebebe208f645e4ce8d0fc2de79357cb9566eff92da3754b66a504568272e705d6403fad2df8112b 6dbc0b1c2f8735d382a39121c5ac11252b591d3fc73dac2b8a8af50408e132cbdb3d28990d8eb1b9e9dd6d8ea1 cc11673c68b23b4c0dd03de1510e19de07e63def97e8f22a9006a5. \quad (7)$$

$$\langle U_2 \rangle = dcf091273ab79b6239ca01c45df069cdbc753e5b913b9173987457e00358b09303d397eb3cf6f22bde0123a39 a1d90e2fff279f7f31934f6bc09fdeb12dc1dfe0aa3ee488e8635c18b034451af657e36218c2f297e98509fd402 6ceec706de389da3087cf5d8ddc1a0d87c34c1ae538ee93cad4e95bf3a205d2a60a5332f3171a462e3ee323b3f e4f3062c4cf03b54d01108e76b46d769f0695c9773a57c84c883e33375a49fece37fe13ea9e24b50adf40bbd2d dc6e55c3a4234cc1868e1056fe80fdf41abcbb48022e44c2daa27d56357c86379de24e6686a8974f6740a4577c f0f02eea8a5ac0ce3e9d37b235105646da800b1d459abd284f14e091304bbc034b89e49dfaed9b0a91701ff23a 5cc032a5649dc311cbb779365ee118a5658875b1ad911a86125be3d0e04e0f0e03e1c71bb694e5e516c1d1adcf 0a7ae48b01a4385f33d345d430177b0cacc2314a89f28ef2a1e25 \quad (8)$$

$$\langle U_3 \rangle = 19f3c4a38e8fff4fc59b105601241f538f9c26667dba60ccc8c964cef5257145ab6d22d9e46164775c18ecd332 73c7e69c9a230ef49d9077dd38c6cead11e97c261b9e61a5e2d5c9689ae23d13bcc640047ca9455cfa6d1853ea 9f2abae547242cc15e99fc3f6ee20b9d68fb86533a9858d82bde04912afcb6bb1c93321f2e614c9c484c89f863 09f3906453b80cb10bf3d384e331c7407b29ba005412c6c11a1f338f06d447cb99ff8036a621c6f67be8e93e55 a35ab7534b3b3d4e0e3cb5f31ccd32684235e5f42ceb343a996e562ff3aa512809794d5a713cc532fc1291873c d5e0e32031ecc9f23d0ed175c6df6f9b95a2586846f6dcd7c8dc0e8aea44a4b47a09a98d8e6e6cb2292fbf8128 e98d06fe769c25ae5367b03d188cd6ad6fa42633e017e433e498ed23a47de0f8e7d4f16de119e9af0e1c7582d5 f1c0dff6f2d347a17504e7cbaf3731b73144fd1f391e1dac75f3e3 \quad (9)$$

$$\langle U_4 \rangle = 41ab52f1cb58c4d9beb4976476d48ba1eb2aad52509c1ba301c624f75a6788527f2811dbafb0caf9bfec32c53 1a268179bde06884cd1d7d22cf83ed26aa476b32deb2bc23bc0834120ed39b32934432393598de3155c96cfe16 1caec77ee8f8d7784e019006a824def13f430a6f8f855eea06af355fff5eb54b6c5545e46b116aabb1e6eb33b2a 3d4b3954bf54a0d68a68e4ba4888c6ba229a4be2a8914d2ff102047ba811f065afa5ea74ddb1f3f6b473a3bf42 e1bd9104f46a4f3ca8547c2dcbb8b6539a46c5bed6bdc68b2863c5cfdb65a65849fd9ae2a15cd37721995126cf deac741ba28bce7f047ac0c6a82a285e3ac1f255b81a2de80d5cdff5afd3d1be718376fe2225248e05b83fd342 e083996639fb17af0934ae78a9f0c2d249051cd23d4f4477f930f9385a6c77348b2217566ef2cdbe675736af16 2cd0e5fbd58c6193a37361498eb407ccf485eef0e41c4e1ba38552 \quad (10)$$

---

[2] Augot, D., Bardet, M., Faugère, J.-C., "On the Decoding of Binary Cyclic Codes With the Newton Identities," *Journal of Symbolic Computation*, V44, N12, PP. 1608-1625, 12/09

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[3] Orsini, E. Sala, M., "Correcting Errors and Erasures Via the Syndrome Variety," *Journal of Pure and Applied Algebra*, V200, N1-2, pp. 191-226, 8/05.

[4] Orsini, E. Sala, M., "General Error Locator Polynomials for Binary Cyclic Codes With $t \leq 2$ and $n < 63$," *IEEE Trans. on Information Theory*, V53, N3, pp. 1095-1107, 3/07.

[5] Truong, T.K., Shih, P.Y., Su, W.K., Lee, C.D., Chang, Y., "Algebraic Decoding of the (89, 45, 17) Quadratic Residue Code," *IEEE Trans. on Information Theory*, V54, N11, pp. 5005-5011, 11/08.

[6] Chang, Y., Lee, C.D., "Algebraic Decoding of a Class of Binary Cyclic Codes Via Lagrange Interpolation Formula," *IEEE Trans. on Information Theory*, V56, N1, pp. 130-139, 1/10.

[7] Truong, T.K., Chang, Y., Lee, C.D., "The Weight Distributions of Some Quadratic Residue Codes," *IEEE Trans. on Information Theory*, V51, N5, pp. 1776-1782, 5/05.

[8] Musa, M.B., "On Some Double Circulant Binary Extended Quadratic Residue Codes," *IEEE Trans on Information Theory*, V54, N2, pp. 898-905, 2/08.

[9] Helleseth, T., Voloch, J.F., "Double Circulant Quadratic Residue Codes," *IEEE Trans on Information Theory*, V50, N9, pp. 2154-2155, 9/04.

[10] Reed, I.S., Truong, T.K., Chen, X., Yin, X., "The Algebraic Decoding of the (41, 21, 9) Quadratic Residue code," *IEEE Trans on Information Theory*, V38, N3, pp. 974-986, 5/92

[11] Lin, T.C., Truong, T.K., Lee, H.P., Chang, H.C., "Algebraic Decoding of the (41, 21, 9) Quadratic Residue Code," *Information Sciences*, V179, N19, pp. 3451-3459, 9/09

[12] Chen, Y.H., Lee, C.D., Chen, Y.H., Tai, S.H., "Efficient Decoding of Systematic (41, 21, 9) Quadratic Residue Code," *IEEE Asia-Pacific Services Computing Conference*, Yilin, Taiwan, pp. 128-133, 12/08

[13] Lee, C.D., Chen, Y.H., "A Decoding Method for Binary Quadratic Residue Codes," *The 14th Asia-Pacific Conference on Communications*, Toyko, Japan, 10/08

[14] Su, W.K., Shih, P.Y., Lin, T.C., Truong, T.K., "A Modified Algorithm for Decoding the (41, 21, 9) Quadratic Residue Code," *IEEE VTS Asia Pacific Wireless Communications Symposium*, Sendai, Japan, 8/08

[15] Su, W.K., Shih, P.Y., Lin, T.C., Truong, T.K., "Decoding of the (41, 21, 9) Quadratic Residue Code Using the Gao's Algorithm," *International MultiConference of Engineers and Computer Scientists*, Hong Kong, China, 3/08

[16] Chen, Y.H., Truong, T.K., Huang, C.H., Chien, C.H., "A Lookup Table Decoding of Systematic (47, 24, 11) Quadratic Residue Code," *Information Sciences*, V179, N14, pp. 2470-2477, 6/09

[17] Lidl, R., Niederreiter, H., *Introduction to Finite Fields and Their Applications*, Cambridge Univ. Press, 1986.

ISBN: 978-988-18210-4-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)