Proceedings of the International MultiConference of Engineers and Computer Scientists 2011 Vol I,
IMECS 2011, March 16 - 18, 2011, Hong Kong

Algebraic Decoding of Two Quadratic Residue Codes Using Unknown Syndrome Representation

Jin-Hao Miao and Chong-Dao Lee *

Abstract—**This paper addresses the problem of improving the unknown syndrome representations to develop algebraic decoding of the (17,9,5) and (23,12,7) binary quadratic residue codes up to true minimum distance, respectively. The proposed unknown syndrome representations are expressed as binary polynomials in terms of the single known syndrome, which is different from the known syndrome in [Chang-Lee, Algebraic decoding of a class of binary cyclic codes via Lagrange interpolation formula, IEEE Trans. Inf. Theory, 2010]. Programs written in C++ language have been executed to obtain the optimal unknown syndrome representations for these two quadratic residue codes.**

Keywords: quadratic residue code, unknown syndrome representation

1 Introduction

The binary block code with length 23 and error-correcting capacity 3 was first introduced by Golay [1] in 1949. The Golay code, which is also a binary quadratic residue code, has been widely used in deep space communication[2]. In 1987, an efficient decoding algorithm of binary Golay code was introduced by Elia [3]. This algebraic algorithm consist of three steps. First, calculate the known syndromes. Next, determine the error locator polynomial. Finally, find the roots of the error locator polynomial. In order to reduce decoding time, the shift-search method [4] is applied to decode three errors of the Golay code. Recent research on decoding binary quadratic residue code is based on Zech logarithmic calculation [5], syndrome-weight determination [6], lookup table [7], unknown syndrome [8], and general error locator polynomial [9]-[10].

The aim of this paper is to develop algebraic decoding of the (17,9,5) and (23,12,7) binary quadratic residue codes based on the proposed unknown syndrome presentations. These results have been verified by software simulation. Programs in C++ language have been executed to check all correctable patterns for the two quadratic residue codes. Moreover, the computational complexity of the developed decoding algorithm is slightly reduced.

*J.-H. Miao and C.-D. Lee are Departments of Information and Communication Engineering, respectively, I-Shou University, Taiwan, R.O.C. Tel/Fax: 886-7-6577711/6578930 Emails: {isu9903004m,chongdao}@isu.edu.tw

2 (17,9,5) Quadratic Residue Code

Throughout this paper, let $\mathbb{F}_2 = \{0, 1\}$. The *quadratic residue set* $Q_{17} = \{j^2 \pmod{17} \mid j = 1,\ 2, ..., 16\} = \{1, 2, 4, 8, 9, 13, 15, 16\}$ is the collection of all nonzero quadratic residues modulo 17. Moreover, the set Q_{17} is exactly a cyclotomic coset modulo 17, denoted by $C_1 = \{1 \times 2^j \mid j = 0,\ 1, ..., 7\}$. The (17, 9, 5) binary quadratic residue code C is the double-error-correcting cyclic code generated by the polynomial $g(x) = \prod_{i \in Q_{17}}(x - \beta^i)$, where $\beta = \alpha^{15}$ is a primitive 17th root of unity in the finite field $\mathbb{E} = \mathbb{F}_{2^8}$.

Traditionally, the syndrome S_i is defined to be $S_i = (\beta^{l_1})^i + (\beta^{l_2})^i + \cdots + (\beta^{l_v})^i$, where β^{l_j} for $1 \le j \le v$ are called the *error locators* and $v \le 2$. For a binary quadratic residue code of length n, there is an obvious relation among syndromes, namely, $S_{2i} = S_i^2$, with sub-indices modulo n, if necessary. This implies that $S_2 = S_1^2$ and $S_4 = S_1^4$ for arbitrary binary quadratic residue code.

Let the code polynomial $c(x) = c_0 + c_1 x + \cdots + c_{16}x^{16}$, $c_i \in \mathbb{F}_2$, be transmitted through a noisy channel to obtain the received polynomial of the form $r(x) = c(x) + e(x)$, where $e(x) = e_0 + e_1 x + \cdots + e_{16}x^{16}$, $e_i \in \mathbb{F}_2$, is an error polynomial. The *known syndromes* S_i, $i \in Q_{17}$ can be obtained by evaluating $r(x)$ at the roots of the generator polynomial $g(x) = 1 + x^3 + x^4 + x^5 + x^8$, i.e.,

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

On the other hand, the other syndromes S_k, where $k = 3, 5, 6, 7, 10, 11, 12, 14$, are called the *unknown syndromes*.

It was shown in [8] that the finite field version of Lagrange interpolation formula found in [11] is employed to derive the unified representation for the primary unknown syndrome S_3. For the (17,9,5) binary quadratic residue code, the unknown syndrome S_3 can be expressed as a polynomial function in terms of the first known syndrome S_1, i.e. $S_3 = S_1^3(1 + (S_1^{17})^3 + (S_1^{17})^5 + (S_1^{17})^6 + (S_1^{17})^7)$. Furthermore, it is interesting to know the unified representations for the other unknown syndromes S_5, S_6, S_7, S_{10}, S_{11}, S_{12}, and S_{14}. Lagrange interpolation method has been verified by software simulation by a computer. Programs in C++ language have been executed to derive all unknown syndrome representations listed in Table 1. From this table, it is easy to see that the unknown syndrome

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table 1: Unknown Syndrome Representations for the (17, 9, 5) Quadratic Residue Code

unknown syndrome	polynomial representation	weight	degree	note
S_3	$S_1^3 + S_1^{54} + S_1^{88} + S_1^{105} + S_1^{122}$	5		[8]
S_5	$S_1^5 + S_1^{39} + S_1^{56} + S_1^{73} + S_1^{124}$	5		
S_6	$S_1^6 + S_1^{40} + S_1^{74} + S_1^{91} + S_1^{108}$	5		
S_7	$S_1^7 + S_1^{24} + S_1^{75} + S_1^{109} + S_1^{126}$	5		
S_{10}	$S_1^{61} + S_1^{95} + S_1^{112}$	3		
S_{11}	$S_1^{11} + S_1^{62} + S_1^{79} + S_1^{96} + S_1^{113} + S_1^{130} + S_1^{147}$	7		
S_{12}	$S_1^{46} + S_1^{63} + S_1^{80}$	3	lowset	optimal
S_{14}	$S_1^{14} + S_1^{31} + S_1^{48} + S_1^{82} + S_1^{116} + S_1^{133} + S_1^{150}$	7		

S_{12} is expressed as a polynomial of the lowest degree 80 and weight 3. Such a polynomial is optimal in algebraic decoding of the (17,9,5) quadratic residue code. The computational complexities of the unknown syndromes S_3 and S_{12} are compared in respect of the numbers of finite field additions/multiplications and shift cycles as shown in Table 2.

Now we are ready to propose an algebraic decoding of the (17,9,5) binary quadratic residue code. The proposed algorithm consists of three steps. In Step 2, the Inverse-Free Berlekamp-Massey Algorithm (IFBMA) is used to efficiently determine the error locator polynomial of a cyclic code. For more detailed procedures, see Appendix.

Input: $r(x)$. **Output:** $c(x) = r(x) - e(x)$.

1. *Syndrome Calculation*
   $S_1 = r(\beta)$, $S_2 = S_1^2$, $S_4 = S_2^2$,
   $S_{12} = S_1^{12}(S_1^{17})^2(1 + S_1^{17} + (S_1^{17})^2)$, $S_3 = S_{12}^{64}$.
2. *Inverse-Free Berlekamp-Massey Algorithm*
   $\sigma(z) =$IFBMA(S_1, S_2, S_3, S_4).
3. *Chien Search Method*
   $e(x) = 0$
   for k from 0 to 16 do
   if $\sigma(\beta^{-k}) = 0$ then $e(x) = e(x) + x^k$

---

3 (23,12,7) Quadratic Residue Code

The set of quadratic residues modulo 23 defined in Section 2 is $Q_{23} = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. Let $\beta = \alpha^{89}$ be a primitive 23rd root of unity in $\mathbb{E} = \mathbb{F}_{2^{11}}$. If α is a root of the primitive polynomial $p(x) = 1 + x^2 + x^3 + x^4 + x^8$, then the generator polynomial of the (23,12,7) quadratic residue code is $g(x) = \prod_{i \in Q_{23}}(x - \beta^i) = 1 + x + x^2 + x^4 + x^6 + x^7 + x^8$. Denote $I(x) = i_0 + i_1 x + \cdots + i_{11} x^{11}$ by the information polynomial. Utilization of the systematic encoder

$$c(x) = I(x) \cdot x^{11} + [I(x) \cdot x^{11} \bmod g(x)] \tag{2}$$

yields the code polynomial $c(x)$ of degree 23.

In this quadratic residue code, there are eleven unknown syndromes S_k, where k =5,7,10,11,14,15,17,19,20,21,22. In [8], the (23,12,7) binary quadratic residue code possesses the unknown syndrome representation

$$\begin{aligned} S_5 &= S_1^{28} + S_1^{51} + S_1^{74} + S_1^{166} + S_1^{258} + S_1^{281} \\ &\quad + S_1^{304} + S_1^{396} + S_1^{534} + S_1^{580} + S_1^{649} + S_1^{672} \\ &\quad + S_1^{1155} + S_1^{1316} + S_1^{1408} + S_1^{1546} + S_1^{1569} \end{aligned} \tag{3}$$

To decode the (23,12,7) quadratic residue code, we propose the unknown syndrome representation for S_{11} developed in this paper instead of S_5 in [8]. The unknown syndrome S_{11} is a binary polynomial of degree 1184 in terms of the known syndrome S_1 as follows:

$$\begin{aligned} S_{11} &= S_1^{11} + S_1^{34} + S_1^{57} + S_1^{149} + S_1^{172} + S_1^{195} \\ &\quad + S_1^{356} + S_1^{402} + S_1^{448} + S_1^{517} + S_1^{540} + S_1^{586} \\ &\quad + S_1^{609} + S_1^{770} + S_1^{816} + S_1^{1092} + S_1^{1184} \\ &= S_1^{11}(1 + (S_1^{23})^1 + (S_1^{23})^2 + (S_1^{23})^6 + (S_1^{23})^7 \\ &\quad + (S_1^{23})^8 + (S_1^{23})^{15} + (S_1^{23})^{17} + (S_1^{23})^{19} \\ &\quad + (S_1^{23})^{22} + (S_1^{23})^{23} + (S_1^{23})^{25} + (S_1^{23})^{26} \\ &\quad + (S_1^{23})^{33} + (S_1^{23})^{35} + (S_1^{23})^{47} + (S_1^{23})^{51}). \end{aligned} \tag{4}$$

The computational complexities of the unknown syndromes S_5 and S_{11} are compared in respect of the numbers of finite field additions/multiplications and shift cycles as shown in Table 2.

The received word is really a codeword if the known syndrome S_1 calculated by the received polynomial is zero. If S_1 is not equal to zero, then the errors occur in the received word and the following decoding algorithm to decode (23,12,7) quadratic residue code is needed. This algorithm consists of three steps.

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table 2: Complexity of Unknown Syndrome Representations for Two Quadratic Residue Codes

code length	unknown syndrome	addition	multiplication	shift
17	S_3	4	7	6
	S_{12}	2	5	5
23	S_5	16	25	6
	S_{11}	16	24	6

Input: $r(x)$. **Output:** $c(x) = r(x) - e(x)$.

1. *Syndrome Calculation*
   $S_1 = r(\beta)$, $S_2 = S_1^2$, $S_4 = S_2^2$, $S_3 = S_4^{64}$, $S_6 = S_3^2$, S_{11} in (4), $S_5 = S_{11}^{128}$.
2. *Inverse-Free Berlekamp-Massey Algorithm*
   $\sigma(z) =$IFBMA$(S_1, S_2, S_3, S_4, S_5, S_6)$.
3. *Chien Search Method*
   $e(x) = 0$
   for k from 0 to 22 do
   if $\sigma(\beta^{-k}) = 0$ then $e(x) = e(x) + x^k$

---

4 Conclusions

This paper has presented the optimal unknown syndrome representation to slightly improve algebraic decoding of two binary quadratic residue codes up to actual minimum distance.

Acknowledgment

The work was supported by National Science Council, R.O.C., under Grant NSC99-2221-E-214-051-MY3.

Appendix

Inverse-Free Berlekamp-Massey Algorithm: The symbol $C^{(k)}(x)$ is defined to be the error-locator polynomial in the stage k. The known syndrome S_k will be used to calculate the discrepancy $\triangle^{(k)}$. The symbols $A^{(k)}(x)$, $\ell^{(k)}$, and $\eta^{(k)}$ are auxiliary variables for finding the error-locator polynomial at the same stage. The five steps of the IFBMA are given as follows.

Step 1) Initialize $k = 1$, $\eta^{(0)} = 1$, $C^{(0)}(x) = 1$, $A^{(0)}(x) = 1$, and $\ell^{(0)} = 1$.

Step 2) Compute the discrepancy

$$\triangle^{(k)} = \sum_{j=1}^{\ell^{(k-1)}} c_{j-1}^{(k-1)} S_{k-j+1}.$$

Step 3) Compute the error-locator polynomial

$$C^{(k)}(x) = \eta^{(k-1)} C^{(k-1)}(x) - \triangle^{(k)} A^{(k-1)}(x) \cdot x.$$

Step 4) Transform the auxiliary variables

$$A^{(k)}(x) = \begin{cases} x \cdot A^{(k-1)}(x), & \text{if } \triangle^{(k)} = 0 \text{ or } 2\ell^{(k-1)} > k-1 \\ C^{(k-1)}(x), & \text{if } \triangle^{(k)} \neq 0 \text{ and } 2\ell^{(k-1)} \leq k-1 \end{cases}$$

$$\ell^{(k)} = \begin{cases} \ell^{(k-1)}, & \text{if } \triangle^{(k)} = 0 \text{ or } 2\ell^{(k-1)} > k-1 \\ k - \ell^{(k-1)}, & \text{if } \triangle^{(k)} \neq 0 \text{ and } 2\ell^{(k-1)} \leq k-1 \end{cases}$$

$$\eta^{(k)} = \begin{cases} \eta^{(k-1)}, & \text{if } \triangle^{(k)} = 0 \text{ or } 2\ell^{(k-1)} > k-1 \\ \triangle^{(k)}, & \text{if } \triangle^{(k)} \neq 0 \text{ and } 2\ell^{(k-1)} \leq k-1 \end{cases}$$

Step 5) Update index number $k = k + 1$ if $k < 2t$, then return Step 2). Otherwise, stop.

References

[1] Golay, M.J.E., "Notes on Digital Coding," *Proc. IRE*, V37, p. 657, 6/49.

[2] Baumert, L.D., McEliece, R.J., "A Golay-Viterbi Concatenated Coding Scheme for MJS'77," *JPL Tech. Report* 32-1526, V18, pp. 76-84, /73.

[3] Elia, M.,"Algebraic decoding of the (23, 12, 7) Golay code," *IEEE Trans. Information Theory*, V33, pp. 150-151, 1/87.

[4] Reed, I.S., Yin, X., Truong, T.K., Holmes, J.K., "Decoding the (24, 12, 8) Golay code," *Proc. IEE*, V137, pp. 202-206, 5/90.

[5] Lee, C.D., "Zech Logarithmic Decoding of Triple-Error-Correcting Binary Cyclic Codes," *IEEE Commun. Lett.*, V12, pp. 776-778, 10/08.

[6] Chang, Y., Lee, C.D., Chen, Z.H., Chen, J.H., "(23,12,7) quadratic residue decoder based on syndrome-weight determination," *Elect. Lett.*, V44, pp. 1147-1149, 11/08.

[7] Chen Y.H., Chien, C.H., Huang, C.H., Truong, T.K., Jing, M.H.,"Efficient Decoding of Systematic (23, 12, 7) and (41, 21, 9) Quadratic Residue Codes," V26, pp. 1831-1843, 9/10.

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table 3: Unknown Syndrome Representations for the (23, 12, 7) Quadratic Residue Code

unknown syndrome	polynomial representation	weight	degree	note
S_5	$S_1^{28} + S_1^{51} + S_1^{74} + S_1^{166} + S_1^{258} + S_1^{281}$ $+S_1^{304} + S_1^{396} + S_1^{534} + S_1^{580} + S_1^{649} + S_1^{672}$ $+S_1^{1155} + S_1^{1316} + S_1^{1408} + S_1^{1546} + S_1^{1569}$	17		[8]
S_7	$S_1^{7} + S_1^{53} + S_1^{76} + S_1^{122} + S_1^{168} + S_1^{214}$ $+S_1^{260} + S_1^{283} + S_1^{306} + S_1^{352} + S_1^{375} + S_1^{444}$ $+S_1^{513} + S_1^{536} + S_1^{628} + S_1^{697} + S_1^{766} + S_1^{789}$ $+S_1^{1180} + S_1^{1203} + S_1^{1272} + S_1^{1364} + S_1^{1594} + S_1^{1617}$	24		
S_{10}	$S_1^{56} + S_1^{102} + S_1^{148} + S_1^{263} + S_1^{332} + S_1^{516}$ $+S_1^{562} + S_1^{585} + S_1^{608} + S_1^{769} + S_1^{792} + S_1^{1045}$ $+S_1^{1068} + S_1^{1091} + S_1^{1160} + S_1^{1298} + S_1^{1344}$	17		
S_{11}	$S_1^{11} + S_1^{34} + S_1^{57} + S_1^{149} + S_1^{172} + S_1^{195}$ $+S_1^{356} + S_1^{402} + S_1^{448} + S_1^{517} + S_1^{540} + S_1^{586}$ $+S_1^{609} + S_1^{770} + S_1^{816} + S_1^{1092} + S_1^{1184}$	17	lowest	optimal
S_{14}	$S_1^{14} + S_1^{106} + S_1^{152} + S_1^{244} + S_1^{313} + S_1^{336}$ $+S_1^{359} + S_1^{428} + S_1^{497} + S_1^{520} + S_1^{566} + S_1^{612}$ $+S_1^{681} + S_1^{704} + S_1^{750} + S_1^{888} + S_1^{1026} + S_1^{1072}$ $+S_1^{1141} + S_1^{1187} + S_1^{1256} + S_1^{1394} + S_1^{1532} + S_1^{1578}$	24		
S_{15}	$S_1^{38} + S_1^{84} + S_1^{176} + S_1^{291} + S_1^{337} + S_1^{452}$ $+S_1^{521} + S_1^{544} + S_1^{705} + S_1^{774} + S_1^{912} + S_1^{1027}$ $+S_1^{1073} + S_1^{1096} + S_1^{1188} + S_1^{1556} + S_1^{1602}$	17		
S_{17}	$S_1^{17} + S_1^{86} + S_1^{178} + S_1^{201} + S_1^{224} + S_1^{270}$ $+S_1^{293} + S_1^{385} + S_1^{408} + S_1^{546} + S_1^{592} + S_1^{1029}$ $+S_1^{1052} + S_1^{1098} + S_1^{1121} + S_1^{1282} + S_1^{1328}$	17		
S_{19}	$S_1^{19} + S_1^{42} + S_1^{88} + S_1^{226} + S_1^{272} + S_1^{387}$ $+S_1^{456} + S_1^{548} + S_1^{594} + S_1^{778} + S_1^{801} + S_1^{1169}$ $+S_1^{1192} + S_1^{1284} + S_1^{1376} + S_1^{1537} + S_1^{1560}$	17		
S_{20}	$S_1^{43} + S_1^{89} + S_1^{112} + S_1^{135} + S_1^{204} + S_1^{273}$ $+S_1^{296} + S_1^{526} + S_1^{549} + S_1^{641} + S_1^{664} + S_1^{1032}$ $+S_1^{1124} + S_1^{1170} + S_1^{1216} + S_1^{1538} + S_1^{1584}$	17		
S_{21}	$S_1^{44} + S_1^{67} + S_1^{90} + S_1^{136} + S_1^{182} + S_1^{251}$ $+S_1^{343} + S_1^{389} + S_1^{412} + S_1^{481} + S_1^{504} + S_1^{550}$ $+S_1^{665} + S_1^{688} + S_1^{734} + S_1^{757} + S_1^{780} + S_1^{872}$ $+S_1^{1010} + S_1^{1056} + S_1^{1125} + S_1^{1148} + S_1^{1171} + S_1^{1217}$ $+S_1^{1240} + S_1^{1332} + S_1^{1378} + S_1^{1424} + S_1^{1516} + S_1^{1562}$ $+S_1^{1585} + S_1^{1608}$	32		
S_{22}	$S_1^{22} + S_1^{68} + S_1^{114} + S_1^{137} + S_1^{298} + S_1^{321}$ $+S_1^{344} + S_1^{390} + S_1^{712} + S_1^{804} + S_1^{896} + S_1^{1034}$ $+S_1^{1080} + S_1^{1172} + S_1^{1218} + S_1^{1540} + S_1^{1632}$	17		

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

[8] 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.

[9] 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.

[10] Lee, C.D., Chang, Y., Chang, H.H., Chen, J.H., "Unusual General Error Locator Polynomial for the (23,12,7) Golay Code," *IEEE Commun. Lett.*, V12, p.p. 339-341, 4/10.

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

ISBN: 978-988-18210-3-4
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)