International Journal of Statistics and Applied Mathematics

ISSN: 2456-1452
Maths 2017; 2(5): 10-13

www.mathsjournal.com
Received: 03-07-2017
Accepted: 04-08-2017

Baljodh Singh
P.G. Department of Mathematics, S.G.G.S. Khalsa College, Mahilpur, Hoshiarpur. Punjab, India

Correspondence
Baljodh Singh
P.G. Department of Mathematics, S.G.G.S. Khalsa College, Mahilpur, Hoshiarpur. Punjab, India

Decoding of extended reed-solomon codes

Baljodh Singh

Introduction

RS coding system is based on groups of bits, such as bytes, rather than individual 0s and 1s, taking it particularly good at dealing with bursts of errors: six consecutive but errors, for sample can affect at most two bytes. Thus, even a double-error-correction version of a Reed-Solomon Code can provide a comfortable safety factor. Current implementations of Reed-Solomon Codes in CD technology are able to cope with error bursts as long as 4000 consecutive bits.

In this sub-class of BCH codes, the symbol field GF (q) and the error locator field GF (q^m) are the same, i.e., m = 1. Thus, in this case

$$n = q^m - 1 = q - 1$$

The minimal polynomial on any element β in the same field GF (q) is

$$f_\beta (x) = x - \beta$$

Since the symbol field (sub-field) and the error locator field (extension field) are the same, all the minimal polynomials are linear. The generator polynomial for a t error correcting code will be simply

$$g (x) = LCM [f_1(x) f_2(x), \ldots, f_{2t}(x)]$$
$$= (x - \alpha) (x - \alpha^2) \ldots (x - \alpha^{2t-1}) (x - \alpha^{2t})$$

Hence, the degree of the generator polynomial will always be 2t. Thus, the RS code satisfies
$n - k = 2t$
In general, the generator polynomial of an RS code can be written as

$$g (x) = (x - \alpha^i) (x - \alpha^{i+1}) \ldots (x - \alpha^{2t+i-1}) (x - \alpha^{2t+i})$$

A set of J parity check equations will be defined to be orthogonal on the sum of *i* information positions ($\alpha_1, \alpha_2, \ldots, \alpha_i$) and s other positions ($m_1, m_2, \ldots, m_s$) if a) the coefficients in positions $\alpha_1, \alpha_2, \ldots, \alpha_i$ are in each equation, b) the coefficients in positions $m_1, m_2, \ldots, m_s$ are arbitrary, and c) no other position has more than one nonzero coefficient in the J parity check equations. For example, (3) is a set of J = 4 equations orthogonal on the sum of 2 information positions (1, 3) and 3 other positions (2, 5, 7), where the β_i and the γ_i are arbitrary.

A generalized parity check equation on the sum of i information positions ($\alpha_1, \alpha_2, \ldots, \alpha_i$) and s other positions ($m_1, m_2, \ldots, m_s$) is defined to be an equation which gives the sum of the noise digits in positions $\alpha_1, \alpha_2, \ldots, \alpha_i$ if no errors have occurred in positions $m_1, m_2, \ldots, m_s$. It can be written as

$$\begin{bmatrix} 1 & \beta_1 & 1 & 0 & \beta_2 & \gamma_1 & \beta_3 & 0 & 0 \\ 1 & \beta_4 & 1 & 0 & \beta_5 & 0 & \beta_6 & 0 & \gamma_2 \\ 1 & \beta_7 & 1 & \gamma_3 & \beta_8 & 0 & \beta_9 & 0 & 0 \\ 1 & \beta_{10} & 1 & 0 & \beta_{11} & 0 & \beta_{12} & \gamma_4 & 0 \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \\ a_8 \\ a_9 \end{bmatrix}$$

$C_i (\alpha_1, \alpha_2, \ldots, \alpha_i; m_1, m_2, \ldots, m_s) = A_i$

The Reed-Solomon Codes

The extended Reed – Solomon codes T. Kasami [1963] & J. L. Massey [1960] will be defined to the set of codes of length n = q, whose symbols are selected from GF (q) where $q = p^m$. If α is a primitive element of GF (q), then an n-dimensional vector space is spanned by the set of n linearly independent vectors.

$$\begin{aligned} v_0 &= \alpha^0, \alpha^0, \alpha^0, \quad \cdots \alpha^0 \\ v_1 &= 0, \alpha^0, \alpha^1, \quad \cdots \alpha^{\alpha-2} \\ v_2 &= 0, \alpha^0, \alpha^2, \quad \cdots \alpha^{2(\alpha-2)} \\ &\vdots \quad \vdots \quad \vdots \quad \vdots \\ v_{v-1} &= 0, \alpha^0, \alpha^{(\alpha-1)}, \quad \cdots \alpha^{(\alpha-1)(\alpha-2)} \end{aligned} \tag{5}$$

The vth order extended Reed-Solomon (ERS) code will be defined as the code whose generating matrix is the first (v + 1) of vectors (5). Further, T. Kasami [1960]

$$v_i \cdot v_j = \sum_{s=0}^{q-2} \alpha^{s(i+j)} \qquad i \quad or \quad j \neq 0$$

$= 0$ if $(i + j) \neq q - 1$
$= q - 1$ if $(i + j) = q - 1$

$$v_0 . v_0 = \sum_{s=0}^{q-1} \alpha^0 = 0$$

then it follows that the vth order ERS code and the $\mu = q - v - 2$ order ERS code are dual codes. It follows that the vth order code has minimum distance q – v and its dual code has minimum distance v + 2, because

$$\begin{vmatrix} \alpha^0 & & \cdots & \alpha^0 \\ \alpha^{i_1} & & \cdots & \alpha^{i_{\mu+1}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_{\mu+1}} \\ \vdots & \vdots & & \vdots \\ \alpha^{\mu i_1} & \alpha^{\mu i_2} & \cdots & \alpha^{\mu i_{\mu+1}} \end{vmatrix} \neq 0 \quad if \ i_i \neq i_k \ all \ j \ and \ k$$

and all sets of $\mu + 1$ different columns of the parity check matrix are linearly independent.

We will define a code to be completely threshold decodable if there exists a decoding circuit consisting of threshold gates which is capable of correcting at least as many errors as the minimum distance guarantees the code will correct. If the ERS codes are completely threshold decodable by orthogonalizing them, then J = d – 1 = q – v – 1 for the vth order code. Since the dual code has minimum distance v + 2, Theorem 1 gives

$$v + 2 \leq \left\lceil i + \left(\frac{q - i}{q - v - 1} \right), 2 \left(\frac{q - 1}{q - v - 1} \right) \right\rceil_{min} \tag{6}$$

as a necessary condition. For i = 1 (which means the code is completely orthogonalizable or one step orthogonalizable [1], inequality (6) is satisfied when v = 0 or v = q – 2 but not for any other values of v. For v = 0, the number of information position is k = 1; and it is true that any linear code with k = 1 can be completely orthogonalized. In addition, v = q – 2 means d = 2 and complete orthogonalization requires J = d – 1 = 1 parity check equation. Since any linear code with $d \geq 2$ has at least one parity check equation involving each information position, these codes are all completely orthogonalizable. Thus, except for these trivial codes the ERS codes are not completely orthogonalizable.

For i > 1 the situation is not improved much. While the first term in the bracket of inequality (6) increases with i, the second term decreases, and since the smaller of the two is the one selected, we have

$$v + 2 \leq 2 \left\lceil \frac{q - i}{q - v - 1} \right\rceil$$

$$< 2 \left\lceil \frac{q - 1}{q - v - 1} \right\rceil, \qquad i > 1 .$$

This inequality becomes an equality when v = 0 and v=q–3 if q is odd. Since relation (7) is a strict inequality, it follows that the allowable range of v is v > q – 3 or $v \geq q - 2$. This range of v is almost identical to the case i = 1, and it follows then that the ERS codes cannot be completely threshold decoded by L-step orthogonalization for any value of L.

Theorem – 1

A necessary condition for the existence of a set of J parity checks orthogonal on the sum of i information positions for a linear code of length n is that the dual code must have minimum distance less than or equal to the minimum of i + [n – i/J] and 2[n – 1/J]

Theorem – 2

A generalized parity check can be determined on $\alpha_1, \alpha_2, \ldots, \alpha_i$ and $m_1, m_2, \ldots, m_s$ from a set of J parity check equations orthogonal on the sum of the *i* positions $\alpha_1, \alpha_2, \ldots, \alpha_i$ and the s other positions $m_1, m_2, \ldots, m_s$ if [J/2] or fewer errors occur.

Proof: The J parity check equations will be evaluated and A_i will be selected as that value which occurs in more than half

of the equations. A_i will be assigned the value "blank" if J is odd and no value occurs in more than half of the equations. A_i will be assigned the value 0 if J is even and zero (0) occurs in half of the equations, while if any other value appears in half of the equations, A_i will be assigned the value "blank". The proof now follows immediately, since if no errors occurs in $\alpha_1, \alpha_2, \ldots, \alpha_i$ and $m_1, m_2, \ldots, m_s$ then at most [J/2] equations will be in error and at least J – [J/2] will be correct (have a value 0). Thus, whether J is even or odd, 0 will be selected. If some of the errors occur in positions $\alpha_1, \alpha_2, \ldots, \alpha_i$ but none in $m_1, m_2, \ldots, m_s$, then less than [J/2] of the equations will be in error and more than J – [J/2] equations will be correct. Since this latter number is more then half, the decision rule will select the correct value.

Theorem - 3

A generalized parity check equation on the sum of *i* information positions and s other positions $(m_1, m_2, \ldots, m_s)$ can be constructed from a set of J generalized parity checks on the sum of the same *i* information positions and s + 1 other positions which include $m_1, m_2, \ldots, m_s$ if [J/2] or fewer errors have occurred provided no two of the J generalized parity checks involve the same s + 1 other positions.

Proof: The hypothesis of the theorem gives the following generalized parity checks.

$$C_1(\alpha_1, \alpha_2, ..., \alpha_i; m_1, m_2, ..., m_s, m_{s+1}^{(1)}) = A_1$$

$$C_2(\alpha_1, \alpha_2, ..., \alpha_i; m_1, m_2, ..., m_s, m_{s+1}^{(2)}) = A_2$$

$$\vdots$$

$$C_J(\alpha_1, \alpha_2, ..., \alpha_i; m_1, m_2, ..., m_s, m_{s+1}^{(J)}) = A_J$$

where all of the $m_{s+1}^{(i)}$ are different. We must determine a value B such that

$$C(\alpha_1, \alpha_2, ..., \alpha_i; m_1, m_2, ..., m_s) = B$$

The value for B will be that value obtained by the majority of the A_i. If J is even and no value is obtained in a majority of the equations, but zero (0) is obtained in half of the equations, B will be assigned the value of 0. In all other cases B will be assigned the value "blank". The proof now follows immediately, since if no errors occur in $\alpha_1, \alpha_2, \ldots, \alpha_i$ and $m_1, m_2, \ldots, m_s$, then at most [J/2] A_i will be in error (if [J/2] of the $m_{s+1}^{(i)}$ are error locations) and at least J – [J/2] will be correct (have value 0). Thus, whether J is even or odd, 0 will be selected for B. If some of the errors occur in position $\alpha_1, \alpha_2, \ldots, \alpha_i$ but none occur in $m_1, m_2, \ldots, m_s$, then less than [J/2] A_i will be correct. Since this latter number is more than half, the decision rule will select the correct value for B.

Theorem – 4

The sum of the noise digits in positions $\alpha_1, \alpha_2, \ldots, \alpha_i$ and can be determined exactly if [J/2] or fewer errors occur and a set of J parity check equations orthogonal on the i information positions $(\alpha_1, \alpha_2, \ldots, \alpha_i)$ and $(m_1, m_2, \ldots, m_{s-1}, m_s)$ to be constructed from which a generalized parity check can be found (Theorem 2). Further m, may take on J – 1 other different values so that a set of J generalized checks can be constructed from which a generalized check on $(\alpha_1, \alpha_2, \alpha_i)$ and $(m_1, m_2, \ldots, m_{s-1})$ can be found (Theorem 3). Repeated applications of Theorem 3 will finally result in a generalized check on $\alpha_1, \alpha_2, \ldots, \alpha_i$ which is a statement of the theorem.

Theorem 5

The vth order ERS code can be completely threshold decoded by a threshold logic circuit of v + 1 levels.

Proof: If i = 1, the theorem will be proved (by using Theorem 4) if J = d – 1 equations orthogonal on α_1 and s_1 other positions can be found for an arbitrary selection of s out of s + d – 1 positions as α_1 takes on values representing each of the information positions and where d = q – v.

Since the set of coefficients in a parity check equation $(b_1, b_2, \ldots, b_n)$, treated as an n – tuple, is in the null space of the code space, we have

$$[b_1, b_2, \ldots, b_4]\, G^T = 0 \qquad (8)$$

where

$$G = \begin{bmatrix} \alpha^0 & \alpha^0 & \alpha^0 & \cdots & \alpha^0 \\ 0 & \alpha^0 & \alpha^1 & \cdots & \alpha^{\alpha-2} \\ 0 & \alpha^0 & \alpha^2 & \cdots & \alpha^{2(\alpha-2)} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & \alpha^0 & \alpha^v & \cdots & \alpha^{v(\alpha-2)} \end{bmatrix} \qquad \ldots (9)$$

The determinant of any set of (v + 1) different columns of (9) is nonzero, and it follows that (8) can be solved for any set of (v + 1) of b, given the values of the remaining (q – v - 1) b. Thus, a set of parity check equations could be constructed, whose coefficients are given by (10), by assigning the value of 1 and 0 to the positions indicated [a total of (q – v – 1) such positions] and solving for the remaining β and α.

$$\begin{bmatrix} \overbrace{1}^{1} & \overbrace{\beta_{11}\beta_{12} \cdots \beta_{1s}}^{s+1} & \alpha_1 & \overbrace{0 \quad 0 \quad \cdots \quad 0}^{q-v-2} \\ 1 & \beta_{21}\beta_{22} \cdots \beta_{2s} & 0 & \alpha_2 \quad 0 \quad \cdots \quad 0 \\ 1 & \beta_{31}\beta_{32} \cdots \beta_{3s} & 0 & 0 \quad \alpha_3 \quad \cdots \quad 0 \\ \vdots & \vdots & & \\ 1 & \beta_{J1}\beta_{J2} \cdots \beta_{js} & 0 & 0 \quad 0 \quad \cdots \quad \alpha_j \end{bmatrix} \qquad (10)$$

In the parity check matrix (10) s + 1 = v + 1, s = v, and J = q - v – 1; so that n = 1 + s + J = q. This is a set of J = q–v–1 = d – 1 equations orthogonal on α_i and s other positions. In addition, since the location of the s coefficients $\beta_{i1}, \beta_{i2}, \ldots, \beta_{is}$ can be chosen arbitrarily in the set of (s + 1) + (q – v – 2) = s + d – 1 positions, the theorem is proved.

As an example, for q = 4 and v = 1 we have

$$G = H = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 1 & \alpha & \alpha^2 \end{bmatrix} \qquad (11)$$

Where α is a primitive element of GF (4). To find the noise in the first position ($\alpha_1 = 1$), we construct the two sets of J = d – 1 = q – v – 1 = 2 parity check equations whose matrices of coefficients are given by (12) and (13)

$$\begin{bmatrix} 1 & \alpha & 0 & \alpha^2 \\ 1 & \alpha^2 & \alpha & 0 \end{bmatrix} \quad (12)$$

$$\begin{bmatrix} 1 & 0 & \alpha^2 & \alpha \\ 1 & \alpha^2 & \alpha & 0 \end{bmatrix} \quad (13)$$

The noise in the first position is determined by a majority test of the results of majority tests applied to (12) and (13).

Conclusions

A necessary condition for the existence of a set of orthogonal parity check equations is presented, and it is demonstrated that the extended Reed-Solomon codes do not satisfy this condition. a generalization of the concept of orthogonal parity checks is developed, and the existence of a threshold logic decoding circuit for these same codes is proved. Since Forney [1966] has shown that the code words in every BCH code are also code words in some Reed-Solomon code with the same guaranteed minimum distance, the decoding scheme presented here for the ERS codes will decode the BCH codes.

References

1. Aho AV, Hopcroft JE, Ullman JD. The Design and Analysis of Computer Algorithms. Reading, MA: Addison-Wesley, 1974.
2. Ar S, Lipton R, Rubinfeld R, Sudan M. Reconstructing algebraic functions from mixed data, SIAM J Comput. 1999; 28(2):488-511.
3. Berlekamp ER, Ramsey JL. Readable erasures improve the performance of Reed-Solomon codes, IEEE Trans. Inform. Theory. 1978; 24:632-633.
4. Berlekamp ER. Algebraic Coding Theory, 2nd ed. Laguna Hills, CA: Aegean Park, 1984.
5. Berlekamp E. Algebraic Coding Theory. New York: McGraw- Hill, 1968.
6. Blahut RE. Theory and Practice of Error Control Codes. Reading, MA: Addison-Wesley, 1983.
7. Bounded distance +1 soft-decision Reed–Solomon decoding, IEEE Trans. Inform. Theory. 1996; 42:704-720.
8. Chien RT. Cyclic decoding procedures for Bose–Chaudhuri–Hoc-quenghem codes, IEEE Trans. Inform. Theory. 1964; 10:357-363.
9. Cohen H. A Course in Computational Algebraic Number Theory, GTM 138. Berlin, Germany: Springer Verlag, 1993.
10. Decoding of Reed-Solomon codes beyond the error-correction diameter, in Proc. 35th Annu. Allerton Conf. Communication, Control and Computing, 1997.