On the Complete Weight Enumerators of Doubly-Extended Reed-Solomon Codes

Toshiyuki KOHNOSU

Department of Engineering Informatics
Faculty of Information Science and Arts
Osaka Electro-Communication University
18-8 Hatsu-cho, Neyagawa-shi, Osaka, 572-8530, Japan
E-mail: kohnosu@kns.osakac.ac.jp

Abstract

The complete weight enumerator (cwe) of a code classifies the set of codewords according to the number of times that each field element appears in each codeword. The cwe gives more information on structure of a code, so it is useful to obtain the cwe. The cwe’s of Reed-Solomon (RS) codes of small dimensions and their extended codes have been shown in [1][2]. It has been discussed the problem of deriving the cwe of RS codes in [3][4]. In this paper, we derive the cwe’s of doubly-extended RS codes of dimensions two and three. As an application of the cwe’s, we show the ordinary Hamming weight enumerator of the binary code obtained from the doubly-extended RS code by replacing each field element with its binary representation.

1. INTRODUCTION

The complete weight enumerator (cwe) of a code classifies codewords by the number of times each field element appeared in each codeword. The cwe gives more information on structure of a code, so it is useful to obtain the cwe. The cwe’s of Reed-Solomon (RS) codes and their extended codes have been shown in [1][2]. It has been discussed the problem of deriving the cwe of RS codes in [3][4]. In this paper, we derive the cwe’s of doubly-extended RS codes of dimensions two and three. As an application of the cwe’s, we show the ordinary Hamming weight enumerator of the binary code obtained from the doubly-extended RS code by replacing each field element with its binary representation.

2. PRELIMINARIES

2.1. Doubly-Extended Reed-Solomon Codes and Their Dual Codes

2.1.1. Reed-Solomon codes and their dual codes

We consider an \((n, k, d)\) RS code over \(GF(2^m)\), where length \(n = 2^m - 1\), dimension \(k\) and minimum distance \(d = 2^m - k\). Let \(RS_b(n, k)\) denote the \((n, k, d)\) RS codes over \(GF(2^m)\) with the generator polynomial

\[
G(x) = \prod_{i=b}^{b+n-k-1} (x - \alpha^i),
\]

where \(\alpha\) is a primitive element of \(GF(2^m)\) and \(b\) is an integer. Then the parity check matrix \(H_{RS_b(n, k)}\) of \(RS_b(n, k)\) is

\[
H_{RS_b(n, k)} = \begin{bmatrix}
1 & \alpha^h & \alpha^{2h} & \cdots & \alpha^{(n-k)h} \\
1 & \alpha^{h+1} & \alpha^{2h+1} & \cdots & \alpha^{(n-k+1)h} \\
1 & \alpha^{h+n-k-1} & \alpha^{2h+n-k-1} & \cdots & \alpha^{(n-1)(h+n-k-1)}
\end{bmatrix}.
\]

The following lemma holds for the dual code \(RS^*_b(n, k)\) of \(RS_b(n, k)\).

Lemma 1 The dual code \(RS^*_b(n, k)\) of \(RS_b(n, k)\) is equal to \(RS_{-b-1}(n, n-k)\). That is, the roots of the generator polynomial of \(RS^*_b(n, k)\) are the inverses of all the nonzero elements of \(GF(2^m)\) which are not roots of the generator polynomial of \(RS_b(n, k)\). □
2.1.2. Extended Reed-Solomon codes and their dual codes

Adding \((0,0,\ldots,0)^T\) to the last column of \(H_{ERS}(n,k)\), where \(T\) denotes the transpose, moreover, adding
\[
(1, \alpha^b, \alpha^{2b-1}, \cdots, \alpha^{(n-1)b-1}, 0, 1)
\]
to the last row, we have an \((n+1, k, n-k+2)\) extended RS code \(ERS_b(n+1, k)\). The parity check matrix is
\[
H_{ERS}(n+1,k) = \begin{bmatrix}
1 & \alpha^{b-1} & \alpha^{2(b-1)} & \cdots & \alpha^{(n-1)(b-1)} & 1 \\
1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & \alpha^{b+n-k-1} & \alpha^{2(b+n-k-1)} & \cdots & \alpha^{(n-1)(b+n-k-1)} & 0 \\
\end{bmatrix}
\]
(3)

\(H_{ERS}(n+1,k)\) is interpreted the parity check matrix as adding \((1,0,\ldots,0)^T\) to the last column of \(H_{ERS-1}(n,k-1)\). So \(ERS_b(n+1,k)\) is able to be regarded as an \((n+1, k, n-k+2)\) lengthened RS code \(LRS_{b-1}(n+1,k)\) whose original code is \(RS_{b-1}(n,k-1)\). That is, the extended RS code \(ERS_b(n+1,k)\) of \(RS_b(n,k)\) is equal to the lengthened RS code \(LRS_{b-1}(n+1,k)\) of \(RS_{b-1}(n,k)\).

We have the following lemma as for the dual code of \(ERS_b(n+1,k)\).

Lemma 2 The dual code \(ERS_b^\perp(n+1,k)\) of \(ERS_b(n+1,k)\) is equal to \(ERS_{b-1}(n+1,k-1)\).

Once again, adding \((0,0,\ldots,0)^T\) to the last column of \(H_{ERS}(n+1,k)\), moreover, adding
\[
(1, \alpha^{b+n-k}, \alpha^{2(b+n-k)}, \cdots, \alpha^{(n-1)(b+n-k)}, 0, 1)
\]
to the last row, we have an \((n+2, k, n-k+3)\) doubly-extended RS code \(DERS_b(n+2,k)\). The parity check matrix is
\[
H_{DERS}(n+2,k) = \begin{bmatrix}
1 & \alpha^{b-1} & \alpha^{2(b-1)} & \cdots & \alpha^{(n-1)(b-1)} & 0 \\
1 & \alpha^b & \alpha^{2b} & \cdots & \alpha^{(n-1)b} & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & \alpha^{b+n-k-1} & \alpha^{2(b+n-k-1)} & \cdots & \alpha^{(n-1)(b+n-k-1)} & 0 \\
\end{bmatrix}
\]
(4)

\(H_{DERS}(n+2,k)\) is interpreted the parity check matrix as adding \((0,0,\ldots,0,1)^T\) to the last column of \(H_{LRS_{b-1}(n+1,k-1)}\). So \(DERS_b(n+2,k)\) is able to be regarded as an \((n+2, k, n-k+3)\) doubly-lengthened RS code \(DLRS_{b-1}(n+2,k)\) of \(RS_{b-1}(n,k-2)\). That is, the doubly-extended RS code \(DERS_b(n+2,k)\) of \(RS_b(n,k)\) is equal to the doubly-lengthened RS code \(DLRS_{b-1}(n+2,k)\) of \(RS_{b-1}(n,k-2)\).

We have the following lemma as for the dual code of \(DERS_b(n+2,k)\).

Lemma 3 The dual code \(DERS_b^\perp(n+2,k)\) of \(DERS_b(n+2,k)\) is equal to \(DERS_{b-1}(n+2,k-2)\).

The parity check matrix \(H_{DERS_b^\perp(n+2,k)}\) is
\[
H_{DERS_b^\perp(n+2,k)} = H_{DERS_{b-1}(n+2,k-2)} = \begin{bmatrix}
1 & \alpha^{-(b-1)} & \alpha^{-(2b-1)} & \cdots & \alpha^{-(n-1)(b-1)} & 1 & 0 \\
1 & \alpha^{-(b-2)} & \alpha^{-(2b-2)} & \cdots & \alpha^{-(n-1)(b-2)} & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
1 & \alpha^{-(b-k+1)} & \alpha^{-(2b-k+1)} & \cdots & \alpha^{-(n-1)(b-k+1)} & 0 & 0 \\
\end{bmatrix}
\]
(5)

2.2. Complete Weight Enumerator

The cwe of a code enumerates codewords according to the number of each element of the field appeared in each codeword. The cwe of a code over \(GF(2^m)\) is defined as follows. Denote the field elements of \(GF(2^m)\) by \(\{\alpha^j| j \in B\}\), where \(B = \{0,1,\ldots,2^m-2\}\) and by convention \(\alpha^0 = 0\). For a codeword \(c = (c_1,c_2,\ldots,c_n)\), let \(w[c]\) be the complete weight of \(c\) defined as
\[
w[c] = Z_0^{S_0}Z_1^{S_1}\cdots Z_{2^m-2}^{S_{2^m-2}},
\]
(6)

where \(Z_j\) is an indeterminate and \(S_j\) is the number of components of \(c\) equal to \(\alpha^j\), so \(\sum_{j \in B} S_j = n\). The cwe of a code \(C\) is defined as
\[
W_C(Z_0,Z_1,\ldots,Z_{2^m-2}) = W_C(\alpha^j) = \sum_{c \in C} w[c].
\]
(7)

As for the Hamming weight enumerators for linear codes, the cwe satisfies the duality theorem[9].

3. MAIN RESULTS

In this section, we show the cwe’s of the doubly-extended RS codes of dimensions two and three.
3.1. The Complete Weight Enumerator for DERS1\((n + 2, 2)\)

The generator matrix \(G_{\text{DER}}(n + 2, 2)\) of DERS1(n + 2, 2) is equal to the parity check matrix \(H_{\text{DER}}(n + 2, 2)\) of DERS1(n + 2, 2), and \(H_{\text{DER}}(n + 2, 2)\) is the parity check matrix \(H_{\text{DER}}(n + 2, 2)\) of DERS1(n + 2, n). DERS1(n + 2, n) is strange in case of taking account of parameters of original RS codes, but we are able to obtain DERS(n + 2, n) formally. The generator matrix \(G_{\text{DER}}(n + 2, 2)\) of DERS1(n + 2, 2) is as follows:

\[
G_{\text{DER}}(n + 2, 2) = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & 0 \\
1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} & 0 & 1
\end{bmatrix}.
\]

The codeword \(c\) corresponding to the message \(a = (a_0, a_1, a_2)\) is obtained by \(aG_{\text{DER}}(n + 2, 2)\), where \(a_0, a_1, a_2 \in GF(2^m)\). If \(a_1 = 0\), the first \(2^m\) symbols of a codeword are \(a_0\) and the last is 0. So the contribution to the cwe in this case is

\[
Z_s \sum_{j \in B} Z_j^{2^m}.
\]

If \(a_1 \neq 0\), the first \(2^m\) symbols of a codeword are all the distinct elements of \(GF(2^m)\) and the last is \(a_1\). For fixed nonzero \(a_1\), the same cwe appears \(2^m\) times according to \(a_0\) and the contribution to the cwe in this case is

\[
2^m \gamma \sum_{j \in B^*} Z_j,
\]

where \(B^* = B \setminus \{\ast\}\) and \(\gamma = \prod_{j \in B} Z_j\).

As the result we have the cwe of DERS1(n + 2, 2) as follows:

**Theorem 1** The cwe of DERS1(n + 2, 2) is given by

\[
W_{\text{DER}}(n + 2, 2)(Z) = Z_s \sum_{j \in B} Z_j^{2^m} + 2^m \gamma \sum_{j \in B^*} Z_j.
\]

3.2. The Complete Weight Enumerator for DERS1(n + 2, 3)

The generator matrix \(G_{\text{DER}}(n + 2, 3)\) of DERS1(n + 2, 3) is equal to the parity check matrix \(H_{\text{DER}}(n + 2, 3)\) of DERS1(n + 2, 3), and \(H_{\text{DER}}(n + 2, 3)\) is the parity check matrix \(H_{\text{DER}}(n + 2, n - 1)\) of DERS1(n + 2, n - 1).

The generator matrix \(G_{\text{DER}}(n + 2, 3)\) of the DERS1(n + 2, 3) is as follows:

\[
G_{\text{DER}}(n + 2, 3) = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 & 1 & 0 \\
1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} & 0 & 0 \\
1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2(n-1)} & 0 & 1
\end{bmatrix}.
\]

Let the message be \(a = (a_0, a_1, a_2)\), where \(a_0, a_1, a_2 \in GF(2^m)\). \(c(a_0, a_1, a_2)\) denotes the codeword whose message is \(a = (a_0, a_1, a_2)\), so \(c(a_0, a_1, a_2) = aG_{\text{DER}}(n + 2, 3)\).

The case of \(a_1 = 0\) is first considered. Since the order of \(\alpha^2\) is \(2^m - 1\), the first \(2^m\) symbols of the last row of \(G_{\text{DER}}(n, 3)\) is all the distinct elements of \(GF(2^m)\). So the cwe of this case can be obtained in the same way as DERS1(n + 2, 2), and equals to \(W_{\text{DER}}(n + 2, 2)(Z)\).

In the case of \(a_1 \neq 0\) and \(a_2 = 0\), the first \(2^m\) symbols of a codeword are all the distinct elements of \(GF(2^m)\) and the last is 0 and the same cwe appears \(2^m(2^m - 1)\) times. So the contribution to the cwe in this case is

\[
2^m(2^m - 1)\gamma Z_s.
\]

In the case of \(a_1 \neq 0\) and \(a_2 \neq 0\), the method in [1] is applicable in the same way as follows. If \(a_1 = a_2 = 1\), \(\eta \in GF(2^m)\) is included in the first \(2^m\) symbols of the codeword on condition that the quadratic polynomial \(y^2 + y + a_0 = \eta\) has two solution in \(GF(2^m)\). \(y^2 + y + a_0 = \eta\) has two solution in \(GF(2^m)\) if only if \(T(a_0) = T(\eta)\), where \(T(\delta)\) denotes the trace of \(\delta \in GF(2^m)\). Let \(B_0 = \{i \mid T(a_i) = 0\}\) and \(B_0^* = B \setminus B_0\). If we define

\[
\beta_0 = \prod_{j \in B_0} Z_j^2,
\]

\[
\overline{\beta}_0 = \prod_{j \in B_0^*} Z_j^2,
\]

then

\[
w[c(a_i, a_j, 1)] = \{\beta_0 Z_0, i \in B_0; \overline{\beta}_0 Z_0, i \in B_0^*\}.
\]

Next we consider the cwe of \(w[c(a_i, a_j, 1)]\). We define translations of the sets \(B_0\) and \(B_0^*\) as \(B_t = \{t + u \mid u \in B_0\}\) and \(B_t^* = \{t + u \mid u \in B_0^*\}\), where \(t = 0, 1, 2, \ldots, 2^m - 2\), addition is modulo \(2^m - 1\) and \(j + \ast = \ast\). Further we define

\[
\beta_t = \prod_{j \in B_t} Z_j^2,
\]

\[
\overline{\beta}_t = \prod_{j \in B_t^*} Z_j^2.
\]
For fixed $a_0 = \alpha^t$, the power of $\alpha$ of elements for the first $2^m$ symbols of the codeword is the set $B_1$ or $B_t$, whose elements contain $i$ and the last symbol of the codeword is 1. So $w[c(\alpha^t, \alpha^t, 1)]$ is

$$w[c(\alpha^t, \alpha^t, 1)] = \left\{ \begin{array}{l} \beta_t Z_0; \\
Z_1 \beta_t Z_0. \end{array} \right. \quad (19)$$

All the sets containing $i$ for $B_t$ or $B_t$ appears one time each when $a_1$ runs through $GF(2^m) \setminus \{0\}$. As the results when $a_0$ runs through $GF(2^m)$ and $a_1$ runs through $GF(2^m) \setminus \{0\}$, $B_1$ or $B_t$ for the first $2^m$ symbols of the codeword equally appears $2^{m-1}$ times each from $B_1 \cup B_t$ since $B_1$ or $B_t$ has $2^{m-1}$ elements. At this point the cwe is

$$2^{m-1} \sum_{t \in B_t} (\beta_t Z_0 + \beta_t Z_0). \quad (20)$$

Finally by consideration of $\alpha^t c(\alpha^t, \alpha^t, 1)$, we have the cwe of the case of $a_1 \neq 0$ and $a_2 \neq 0$ as follows.

$$2^{m-1} \sum_{s \in B_s} \sum_{t \in B_t} (\beta_t Z_s + \beta_t Z_s). \quad (21)$$

As the result we have the cwe of $\text{DER}_S(n + 2, 3)$ as follows:

**Theorem 2.** The cwe of $\text{DER}_S(n + 2, 3)$ is given by

$$W_{\text{DER}_S(n+2,3)}(Z) = W_{\text{DER}_S(n+2,2)}(Z) + 2^m(2^m - 1)Z_s + 2^{m-1} \sum_{s \in B_s} \sum_{t \in B_t} (\beta_t Z_s + \beta_t Z_s). \quad (22)$$

4. The Hamming Weight Enumerator of The Binary Code Obtained from The Doubly-Extended RS Code

The cwe can be applied to the computation of the Hamming weight enumerators for the binary expanded RS codes.

Let $A_i$ be the number of codewords of weight $i$ in a code. For example, from the result of Section 3.1, we have the following corollary for the Hamming weight enumerator of the binary code obtained from $\text{DER}_S(n + 2, 2)$.

**Corollary 1.** The Hamming weight enumerator of the binary code obtained from $\text{DER}_S(n + 2, 2)$ is given by

$$A_{m2^m} = \binom{m}{i}, \quad i = 0, 1, \ldots, m, \quad (23)$$

$$A_{m2^m+1} = 2^m \binom{m}{i}, \quad i = 1, \ldots, m. \quad (24)$$

Notice that the Hamming weight enumerator is independent of the choice of basis for the binary representation of each field element over $GF(2^m)$.

5. CONCLUSIONS

Some results on the cwe’s of doubly-extended RS codes of dimensions two and three have been described. We show an application of the cwe to the ordinary Hamming weight enumerator of the binary codes obtained from the RS code. The cwe of doubly-extended RS codes of dimension four might be obtained by using techniques in [1]. Further studies will be required to obtain the cwe’s for RS codes of larger dimensions and other non-binary codes.

**Acknowledgments**

The author would like to thank Professor Kin-ichiroh Tokiwa of Osaka Sangyo University for fruitful discussions to this work.

**References**


