Decoding Shortened Reed Solomon Codes at Bit Level

Ta-Hsiang Hu
Department of Electrical Engineering, Da-Yeh University, Changhua ,Taiwan 515, R.O.C.
thhu@mail.dyu.edu.tw

Ming-Hua Chang
Department of Electronic Engineering, Jinwen University of Science and Technology, New Taipei City, Taiwan 231, R.O.C
mhchang@just.edu.tw

Abstract: - This study presents a novel means of shortening a Reed Solomon (RS) code at the bit level, yielding only shortened BCH subcodes. With the use of a certain basis, an RS codes over $GF(2^m)$ is mapped onto a binary image[4], which contains *m* concatenated BCH sub-codewords and some glue-vector codewords. With the proposed approach, there only exist some shortened BCH subcode generators in the diagonal entries of the corresponding binary image generator matrix of an RS code. Hence, only binary codewords of shortened BCH subcodes exist in concatenation. When such a codeword is transmitted, BCH decoders or an RS decoder can be adopted at the receiver. In simulations of a BPSK coherent system over AWGN channels, the error performance of BCH algebraic decoding is better than that of RS algebraic decoding. The coding gain between both decoding algorithms becomes obvious as the code rate reduces or the error correcting capability of an RS code increases. At the word error rate 10^{-5}, the code gain can reach as much as 1.5 dB at the code date 0.747. Additionally, with the proposed method for shortening RS codes over GF(2^8), such a shortened RS code can be decoded by two or three BCH decoders in parallel, which greatly reducing the decoding times and computational complexity.

Key-Words: - RS decoding, shorten RS codes, shorten BCH codes, binary images.

1 Introduction

Reed-Solomon (RS) codes have been widely adopted in practical error control applications, such as satellite communications or compact disk digital audio & digital versatile disks, high-definition television (HDTV) or digital audio broadcasting / digital video broadcasting (DAB/DVB). They have been widely accepted mostly because their properties make them uniquely suitable for error correction in a broad spectrum of applications. Perhaps, the most important practical aspect of RS codes is their burst error-correcting capability, which makes them effective against degradation and attractive for applications in fading channels, jamming environments, and recording systems.

According to the necessity of applications, some shortened RS codes are desired. In such applications, the system internal architecture determines the values of coding scheme parameters that are required for error control. Shortening is a technique in which some information symbols are removed from the code in order to reduce its dimensionality. Shortened RS codes retain many salient properties of the mother codes, from which they are derived. A shortened RS code can be formed by setting some information symbols in the mother RS code to zero. Since these inherent all-zero symbols can be regarded as known symbols in the receiver, therefore they need not be transmitted. A shortened cyclic code has at least the same error-correcting capability as the mother code[1][2]. So the code is effectively shortened without altering its minimum distance. In the study[2], if the deleted symbols are treated as erased positions, then the standard errors and erasure decoder for an RS code is adopted to decode shortened version of this same code. Any *k* symbols of an RS code can be used as the message symbols in a systematic representation. Given a code sequence with *k* symbols and $n - k$ erasures (assume *n* is the codeword length), the systematic encoding will give a codeword containing the *k* arbitrary symbols in their input positions and the erasures will has been corrected.

A few studies have developed shortened RS codes [5]-[10]. In two of them[5][6], since shortened RS codes over $GF(2^m)$ have the property of maximum distance separability at the symbol level (1 symbol = *m* bits), they are adopted in the fault-tolerance systems to improve the bit error correction. In two other studies[7][8], a rate-compatible punctured and

shortened RS code is utilized to minimizes packet retransmission or packet loss in network communications. In a fifth study[9], the decoding latency matches the shortened RS code length rather than the mother RS code length. Therefore, the saving in decoding latency can be significant. In another study[10], a way to fold a shortened RS code reduces the probability of erroneous reception. All these studies are completed at the symbol level.

Some studies have addressed RS decoding at the bit level [3-4][11-12][16]. In one of them[3], bit-level soft decision information is used in a proposed RS decoding, which is a sort of maximum likelihood decoding (MLD) with less complexity than trellis decoding. However, it can only be adopted to decode short-length RS codes. In [4], the main contribution of this paper was to present a computationally efficient hybrid reliability-based decoding algorithm for RS codes, which yield the same results as MLD. This hybrid decoding algorithm consists of two major components – a re-encoding process and a successive erasure-and-error decoding process for both bit and symbol levels. One study[11] presents a concatenated turbo coding system in which an RS outer code is concatenated with a binary turbo inner code. Since there is an interactive turbo-coding system used in the communication scheme, both encoding and decoding are carried out in two stages, which consist of turbo-decoding and RS decoding with Chase-GMD algorithm. Another investigation[12] proposed an approach to combine both Chase-2[19] and GMD[18] algorithms. This approach generalizes the results of from binary codes to the nonbinary case. It has shown that a Chase-GMD decoder succeeds whenever a GMD decoder does. That study also considered the choices of reliability measures to be used in conjunction with the Chase-GMD algorithm. Another work[16] used the properties of a binary image generator matrix of an RS code to develop a partition decoding algorithm. Simulations reveal that the decoding performance of the proposed partition decoding algorithm is a little poorer, by 1.0 to 1.4 dB at BER 10^{-5}, than that achieved by MLD, but is 0.8 to 1.1 dB better than that achieved by GMD.

No study has yet discussed an algorithm for decoding shortened RS codes at the bit level. Accordingly, an opportunity still exists to increase the effectiveness of decoding by reducing the complexity of decoding a shortened RS codes. In this study, BCH algebraic decoding is adopted for shortened RS codes at the bit level, to increase the error performance than conventional RS algebraic decoding. Additionally, the complexity of decoding a binary BCH code is much less than that of decoding an RS code of the same code length. Based on the motivation of increasing error performance and decreasing decoding complexity of a shortened RS code, a proposed method for shortening RS codes are prevented in this work. In the organization of this work, Section 2 introduces the code structure of binary images of RS codes. Section 3 presents a method for shortening RS codes at the bit level. Based on the code structure of a shortened RS code at the bit level, BCH algebraic decoding is applied to decode such a shortened RS code at the bit level. Section 4 presents simulations and bounds on its error performance. Finally, Section 5 draws conclusions.

2 Code structures of RS codes at bit level

Let C be an (N, K, D) RS code over $GF(2^m)$ with code length N, information length K and minimum distance $D = N - K + 1$. For binary transmission, the symbols of this code must map into binary bits. Let $B = (\beta_0, \beta_1, \cdots \beta_{m-1})$ be a basis of $GF(2^m)$. For a codeword $\overline{V} = (V_0, V_1, \cdots, V_{N-1}) \in C$, each $V_i = a_{i,0}\beta_0 + a_{i,1}\beta_1 + \cdots a_{i,m-1}\beta_{m-1}$ is a symbol in $GF(2^m)$ and each $a_{i,j}$ is a bit in $GF(2)$. Let $\Omega(\overline{V})$ be a mapping that maps a codeword into the following binary mN-tuple,

$$\begin{aligned}\overline{v} &= \Omega(\overline{V}) \\ &= (a_{0,0}, a_{1,0}, \cdots; a_{N-1,0}, a_{0,1}, a_{1,1}, \cdots; a_{N-1,1}, \cdots; a_{0,m-1}, a_{1,m-1}, \cdots a_{N-1,m-1})\end{aligned} \quad (1)$$

The set of binary mN-tuples, $C^{(b)} = \{\overline{v} = \Omega(\overline{V}), \overline{V} \in C\}$, is called the binary image[4][13] of C with respect to B, which is a linear (mN, mK) code with minimum distance $D^{(b)}$ of greater than or equal to D. Conversely, if $\overline{v} \in C^{(b)}$ is known, then the inverse mapping $\Omega^{-1}(\overline{v})$ yields the corresponding codeword $\overline{V} \in C$. Consider an (N, K) RS code with the generator polynomial $g(X) = g_0 + g_1 X + \cdots + g_{N-K} X^{N-K}$; the generator matrix of this code is shown as follows[1],

$$G=\begin{bmatrix} g_0 & g_1 & g_2 & \cdots\cdots & g_{N-K} & 0 & 0 & \cdots\cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots\cdots & g_{N-K} & 0 & \cdots\cdots & 0 \\ 0 & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_{N-K} & 0 \cdots 0 \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots\cdots & 0 & g_0 & g_1 & g_2 & \cdots & \cdots & g_{N-K} \end{bmatrix}=\begin{bmatrix} \bar{g}_0 \\ \bar{g}_1 \\ \bar{g}_2 \\ \vdots \\ \bar{g}_{K-1} \end{bmatrix} \quad (2)$$

where, for $0 \le i \le K-1$, a vector $\bar{g}_i=[X^i g(X)]$ is formed by cyclically shifting the vector $\bar{g}_0=[g(X)]$ by i places, and the notation $[p(x)]=(p_0, p_1, \cdots p_{N-1})$, as $p(X)=p_0+p_1X+\cdots+P_{N-1}X^{N-1}$. Then the generator matrix of the binary image $C^{(b)}$ of C is [4][13]

$$G^{(b)}==\begin{bmatrix} \Omega(\beta_0\bar{g}_0) \\ \Omega(\beta_0\bar{g}_1) \\ \vdots \\ \Omega(\beta_0\bar{g}_{k-1}) \\ \vdots \\ \Omega(\beta_{m-1}\bar{g}_0) \\ \Omega(\beta_{m-1}\bar{g}_1) \\ \vdots \\ \Omega(\beta_{m-1}\bar{g}_{k-1}) \end{bmatrix}. \quad (3)$$

The code structure of a binary image of an (*N, K, D*) RS code over $GF(2^m)$ is the sum of a concatenation of *m* binary (*N*, *k, d*) BCH sub-codes and some glue-vector codewords. The binary generator matrix can be expressed as follows[3][4][13],

$$G^{(b)}=\begin{pmatrix} G_{bch}^{(1)} & 0 & \cdots & 0 \\ 0 & G_{bch}^{(2)} & \cdots & 0 \\ & \ddots & & \\ & & & G_{bch}^{(m)} \\ G_{gv}^{(1)} & G_{gv}^{(2)} & \cdots & G_{gv}^{(m)} \end{pmatrix}, \quad (4)$$

where, for $1 \le i \le m$, $G_{bch}^{(i)}$ and $G_{gv}^{(i)}$ are a $k \times N$ BCH generator sub-matrix and an $m(K-k) \times N$ glue-vector generator sub-matrix, respectively. An example is given as follows.

Example 1: Consider (7, 5, 3) RS code over $GF(2^3)$ generated by the polynomial $-\alpha^3+\alpha+1=0$. The generator polynomial of this code is given by $g(X)=(X+\alpha)(X+\alpha^2)=X^2+\alpha^4X+\alpha^3$. Its corresponding vector is $\bar{g}_0=(\alpha^3, \alpha^4, 1, 0, 0, 0, 0)$. The binary generator matrix, based on the polynomial basis $B = (1, \alpha, \alpha^2)$, is given by (Ex.1.1). Through row operations, the above generator matrix becomes such a trellis oriented generator matrix (TOGM) [14] as shown by (Ex.1.2). Although both generator matrices are different, the binary codes that are generated by these two generators are identical, because of their linearity.

3 Method for shortening RS codes at bit level

Based on this generator matrix structure in (3), a binary information message $\bar{u}$ can be presented:

$$\bar{u}=\left(\bar{u}^{(1)}, \cdots, \bar{u}^{(m)}, \bar{u}^{(g)}\right), \quad (7)$$

where, for $1 \le i \le m$, an information sub-vector $\bar{u}^{(i)}$ is associated with a BCH generator sub-matrix $G_{bch}^{(i)}$ and the sub-vector $\bar{u}^{(g)}$ is related to a glue-vector generator sub-matrix $G_{gv} \underline{\Delta} \left(G_{gv}^{(1)}, \cdots, G_{gv}^{(m)}\right)$. Let c be a codeword in $C^{(b)}(mN, mK, D)$, its encoding is given by

$$\begin{aligned} c &= \bar{u}G^{(b)} \\ &= \left(\bar{u}^{(1)}, \cdots, \bar{u}^{(m)}, \bar{u}^{(g)}\right)\begin{pmatrix} G_{bch}^{(1)} & 0 & \cdots & 0 \\ 0 & G_{bch}^{(2)} & \cdots & 0 \\ \vdots & 0 & & \vdots \\ & \vdots & & G_{bch}^{(m)} \\ G_{gv}^{(1)} & G_{gv}^{(2)} & \cdots & G_{gv}^{(m)} \end{pmatrix} \end{aligned} \quad (8)$$

According to [2], shortening an information bit is equivalent to deleting its related row and column from the mother code generator matrix. For example, if the first information bit is shortened, then the first row and first column are deleted from the mother code generator matrix. In (4), if the information sub-vector $\bar{u}^{(g)}$ is shortened (or fixed as an all-zero vector), then codewords in this shortened code $C^{(b)}$ are generated through these *m* BCH subcode generator matrices in parallel.

However, if the glue-vector information sub-vector $\bar{u}^{(g)}$ is shortened, then the related *m*(*K* - *k*) rows and columns are deleted from the generator matrix $G^{(b)}$. For example, in Example 1, if the last

three rows and the 13th to 15th columns, related to the information sub-vector $\bar{u}^{(g)}$, are deleted, then the parity check sub-matrix in the third subcode matrix, $G_{bch}^{(3)}$, is also deleted. In such a circumstance, the information sub-vector $\bar{u}^{(3)}$ is forced to be all-zero. In other words, some information bits of a BCH subcode are also forced to shorten in addition to shorten these $m(K - k)$ glue-vector information bits.

A method for shortening information bits that are associated with glue-vector information sub-vector $\bar{u}^{(g)}$ in $G^{(b)}$ is proposed here. After it is applied, only shortened BCH subcodes exist in $C^{(b)}$. These shortened BCH subcodes are called the residual shortened BCH subcodes in this work. When the inverse mapping $\Omega^{-1}(\cdot)$ is applied, these residual shortened BCH subcodes can be transformed into the corresponding mother RS code, from which they are derived. The main contribution of this work is to propose a method for shortening RS codes such that only shortened BCH subcodes are obtained, and then decoding can be completed by BCH decoding.

Let L be the number of shortened symbols in a mother RS code, and l be the number of deleted BCH subcodes, and x (assume $x < m$) be the total number of shortened bits in these residual shortened BCH subcodes. To converse the information length, the number of information bits shortened in $C^{(b)}$ equals the number of shortened symbols in the mother RS code over $GF(2^m)$ multiplied by m,

$$mL = m(K-k) + lk + x, \tag{7}$$

where $m(K - k)$ represents the length of the glue vector information in $C^{(b)}$. To converse the code length, the number of bits that are shortened in $C^{(b)}$ is equal to the number of shortened symbols in C multiplied by m:

$$mL = Nl + x \tag{8}$$

(7)(8) yield the following equation;

$$l = \frac{m(K-k)}{N-k}. \tag{9}$$

If Nl is completely divided by m without a remainder, then

$$L = \frac{Nl}{m}, \tag{10}$$

Otherwise,

$$L = \left\lceil \frac{Nl}{m} \right\rceil, \tag{11}$$

where $\lceil y \rceil$ denotes the least number greater than y. From (8), once the values of L and l are found, then the following equation can be obtained.

$$x = mL - Nl. \tag{12}$$

When the proposed shortening method is applied, the mother (N, K) RS code becomes (N', K') RS code with code length $N' = N - L$ and information length $K' = K - L$. The (N', K') RS code only contains m' residual shortened (n', k') BCH subcodes with code length $n' = N - (x/m')$ and $k' = k - (x/m')$, and $m' = m - l$. Table 1 lists the shortened RS codes in their mother codes over $GF(2^8)$, by using this proposed shortening method. The following example is given for illustrative purposes.

Example 2: In Table 1, consider (255, 239) RS code with 8-error-correcting over $GF(2^8)$. There are eight (255, 191) BCH subcodes with 8-error-correcting are contained in this mother code. With this proposed shortening method, there are 192 symbols shortened in the mother RS code, which is equivalent to shorten six (255, 191) BCH subcodes and six bits in the two residual (255, 191) BCH subcodes. Hence, there are two residual shortened (252,188) BCH codes only contained in the shortened (63, 47) RS codes.

4. BCH algebraic decoding for shortened RS codes at bit level

A. Decoding

After the proposed shortening method applied, the mother (N, K) RS code becomes the shortened (N', K') RS code, which only contained some shortened (n', k') BCH codes. Data are encoded by shortened (N', K') RS code. They are transmitted with BPSK signalling. At the receiver, the received sequence is independently decoded by BCH decoding. Then the inverse mapping $\Omega^{-1}(\cdot)$ is applied, the decoded sequence at the symbol level $\hat{V}$ is output. Let a received sequence be $\bar{r} = (\bar{r}_0, \bar{r}_1, \cdots \bar{r}_{m'-1})$, where $\bar{r}_i = (r_{0,i}, r_{1,i}, \cdots r_{n'-1,i})$ and $0 \le i \le m'-1$. The proposed decoding is presented as follows.

1) Decode each $\bar{r}_i$ using the (N, k) BCH algebraic decoders in parallel and output

$$G^{(b)} = \begin{bmatrix} \Omega(\overline{g}_0) \\ \Omega(\overline{g}_1) \\ \Omega(\overline{g}_2) \\ \Omega(\overline{g}_3) \\ \Omega(\overline{g}_4) \\ \Omega(\alpha\overline{g}_0) \\ \Omega(\alpha\overline{g}_1) \\ \Omega(\alpha\overline{g}_2) \\ \Omega(\alpha\overline{g}_3) \\ \Omega(\alpha\overline{g}_4) \\ \Omega(\alpha^2\overline{g}_0) \\ \Omega(\alpha^2\overline{g}_1) \\ \Omega(\alpha^2\overline{g}_2) \\ \Omega(\alpha^2\overline{g}_3) \\ \Omega(\alpha^2\overline{g}_4) \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

(Ex.1.1)

$$G^{(b)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

(Ex.1.2)

a decoded vector $\hat{v} = (\hat{v}_0, \hat{v}_1, \cdots \hat{v}_{m'-1})$

2) Output the decoded sequence (or codeword) at the symbol level $\hat{V} = \Omega^{-1}(\hat{v})$.

In [1][4], RS decoding comprises four steps, which are evaluation of syndromes, determination of the error-locator polynomial, determination of the roots of the error-locator polynomial, and determination of error values. Binary BCH decoding only uses the first three steps to correct binary random errors. The received sequence can be decoded with several BCH decoders in parallel, which is more effective than RS decoding for decoding such a shortened RS code.

B. Error performance bound

Assume such a shortened RS code is transmitted with BPSK signalling over an AWGN channel with zero mean and variance $\frac{N_0}{2}$. Let R denote the shortened code rate, and E_b be the energy of a BPSK signal per information bit. At a BPSK coherent receiver, the error transition probability p is given by

$$p = \widetilde{Q}(\sqrt{2RE_b / N_0}) = \frac{1}{\sqrt{\pi}} \int_{\sqrt{RE_b / N_0}}^{\infty} \exp(-\lambda^2) d\lambda \quad .(\tag{13}$$

Since t+1 symbol (or bit) errors in such a shortened RS code dominate the error performance of algebraic decoding of both RS code and BCH code, therefore the word error rates achieved with (N, K) RS algebraic decoding and with (n, k) BCH algebraic decoding are bounded by

$$P_{e,RS} \geq \binom{n'}{t+1} (1-(1-p)^{m'})^{(t+1)} ((1-p)^{m'})^{(n'-(t+1))} \tag{14}$$

and

$$P_{e,BCH} \geq \binom{n'}{t+1} p^{(t+1)} (1-p)^{(n'-(t+1))} \tag{15}$$

C. Simulations

This study presented a method for shortening RS codes such that only a few shortened BCH subcodes are included in their binary images. Figures 1 to 6 show the error performance of six shortened RS codes, such as shortened (63, 59)RS code, shortened (63, 55)RS code, shortened (63, 51)RS code, shortened (63, 47)RS code, shortened (95, 77)RS code, and shortened (95, 71)RS code. In these figures, coding gains between both algebraic decoding algorithms are various, and they are dependent on the code rate and the error correcting capability of a shortened RS code. As the coding rate decreases, the coding gain for shortened RS codes increases. At the word error rate 10^{-5}, the coding rates in Figures 1 to 6 are 0.939, 0.873, 0.81, 0.746, 0.815 and 0.747, respectively. The corresponding coding gains are 0.44 dB, 0.72 dB, 0.83 dB, 0.88 dB, 1.5 dB and 1.77 dB. The error performance is also proportional to the error correcting capability of a shortened RS code. For example, the error performance of shorten RS codes with 6 and 8 error corrections in Figures 3 and 4 is much less than that of those codes with error correcting capabilities 9 and 12 in Figures 5 and 6.

5. Conclusion

The main contribution of this work is the development of a method for shortening an RS code such that only its shortened BCH subcodes exist in its binary image. Such a shortened RS code can therefore be decoded by either RS decoding or BCH decoding. The decoding complexity of BCH codes is less than that of RS codes[20] and simulation results show that with BPSK signalling, decoding of BCH codes outperforms that of RS codes. Consequently, when the a proposed method for shortening an RS code is used, BCH decoding adopted in parallel is more effective and powerful than RS decoding to eliminate random errors over AWGN channels.

Acknowledgement

The authors would like to thank the National Science Council of the Republic of China, Taiwan, for financially supporting this research under Contract No. NSC 94-2213-E-212-010.

References:

[1] S. Lin and D. J. Costello, Jr., *Error Control Coding*, Prentice Hall, 2004.

[2] S. B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice Hall, 1995.

[3] A. Vardy and Y. Be'ery, "Bit_Level Soft Decision Decoding of Reed_Solomon Codes," *IEEE Trans. Commun.* Vol. 39, No. 3, March 1991, pp. 440-444.

[4] T. H. Hu and S. Lin, "An Efficient Hybrid Decoding Algorithm for Reed–Solomon Codes Based on Bit Reliability," *IEEE Trans. Commun*. Vol. 51, No. 7, July 2003, pp. 1073-1081.

[5] G. R. Redinbo, L. M. Napolitano, Jr., and D. D. Andaleon, "Multibit Correcting Data Interface for Fault-Tolerant Systems," *IEEE Trans. Computer.* Vol. 42, No. 4, April 1993, pp. 433-446.

[6] L. M. Napolitano, D.D. Andaleon, W.O Shreeve and G. R. Redinbo, "Nibble-based error detection or correction (EDOC) chip ," *Electronics Letters*, Vol. 25, Oct. 1989, pp.1542- 1543.

[7] H. Djandji, "An efficient hybrid ARQ protocol for point-to-multipoint communication and its throughput performance," *IEEE Transaction on Veh. Tech.*, Vol. 48, Sept 1999, pp. 1688-1698.

[8] Y. Xu and T. Zhang, "Variable Shortened-and-Punctured Reed–Solomon Codes for Packet Loss Protection," *IEEE Trans. Broadcasting*, Vol. 48, No. 3, Sept. 2002, pp. 237-245.

[9] Shin-Lin Shieh, Shuenn-Gi Lee and Wern-Ho Sheen, "A low-latency decoder for punctured/shortened Reed-Solomon codes," *IEEE 16th international Symposium on Personal, indoor, and Mobile Radio communications*, Vol. 4, Sept. 2005. , pp.2547-2551.

[10] J. Zhang, and M. A Armand, "On Transformed Folded Shortened Reed-Solomon Codes for the Correction of Phased Bursts," *2005 5th international Conference on information, communications and Signal processing*, Dec. 2005, pp. 1374-1378.

[11] C. Y. Liu, H. Tang, S. Lin, and M. P. C. Fossorier, "An Interactive Concatenated Turbo Coding System," *IEEE Vech. Tech.* Vol. 51, No. 5, Sept 2002, pp. 998-1010.

[12] H. Tang, Y. Liu, M. Fossorier, and S. Lin, "On combining Chase-2 and GMD decoding algorithms for nonbinary block codes," *IEEE Commun. Lett.*, Vol. 5, No. 5, May 2001, pp. 209–211.

[13] T. H. Hu and T. M. Tu, "On Binary Images of Reed-Solomon Codes," *Journal of Chung Cheng Institute of Technology*, Vol. 28, No. 2, 2000, pp.53-72.

[14] G. D. Forney, Jr., "Coset codes II: Binary lattices and related codes," *IEEE Trans. Inform. Theory*, Vol. 34, Sept. 1988, pp. 1152–1187.

[15] Couch, *Digital and Analog Communications,* 3rd edition, Macmillan, 1990.

[16] T. H. Hu, M. H. Chang and I. J. Su, "A Partition Decoding for Reed-Solomon Codes Based on Partial Bit Reliability," *IEICE Transactions on Comm.*, Vol. E90-B, No. 10, Oct. 2007, pp. 2784-2791.

[17] M. H. Chang, "The Studies of Decoding Algorithm for BCH codes, Reed-Solomon Codes and Generalized Reed-Solomon Codes," Ph.D. Dissertation, School of Defense Science, Chung Cheng Institute of Technology, National Defense University, Taiwan, R.O.C. 2008.

[18] G. D. Forney, Jr., "Generalized Minimum Distance Decoding," *IEEE Trans. Inform. Theory*, Vol. IT-12, No. 1, April 1966, pp. 125-131.

[19] D. Chase, "A New Class for Decoding Block Codes with Channel Measurement Information," *IEEE Trans. Inform. Theory*, Vol. IT-18, No. 2, Jan 1972, pp. 170-182.

[20] J. Hong and M. Vetterli, "Simple Algorithm for BCH Decoding ," *IEEE Trans Comm.*, Vol. 43, No. 8, Aug. 1995, pp. 2324-2333.

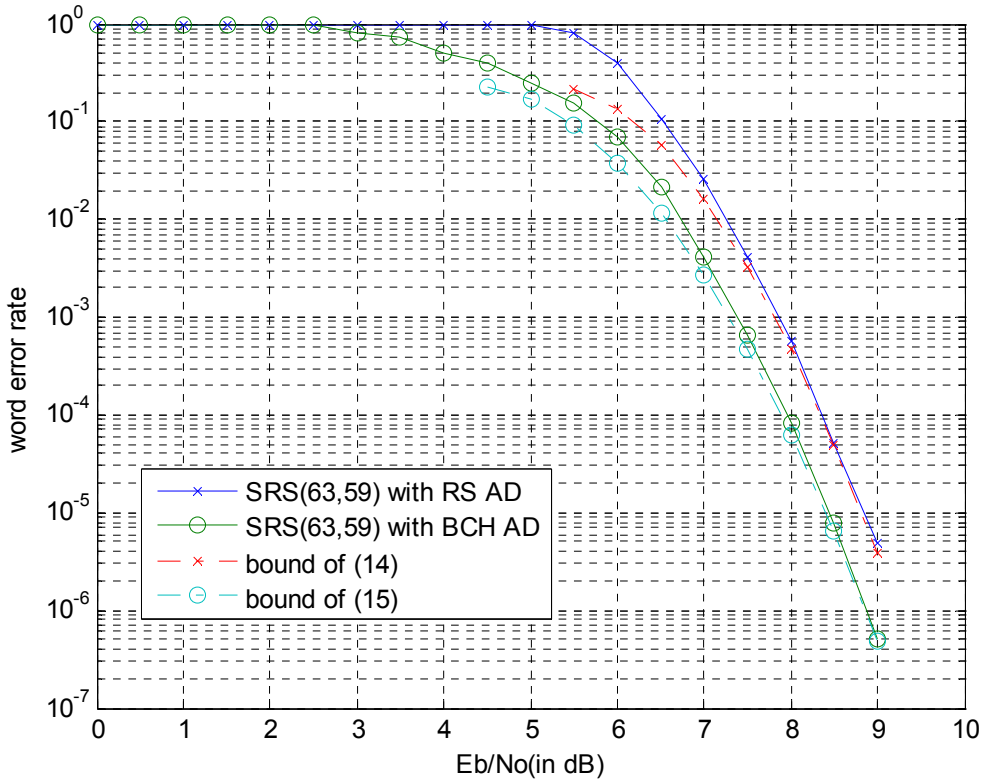


Figure 1: The error performance of RS and BCH algebraic decoding (AD) for a shortened (63, 59) RS code with BPSK coherent system over AWGN channels

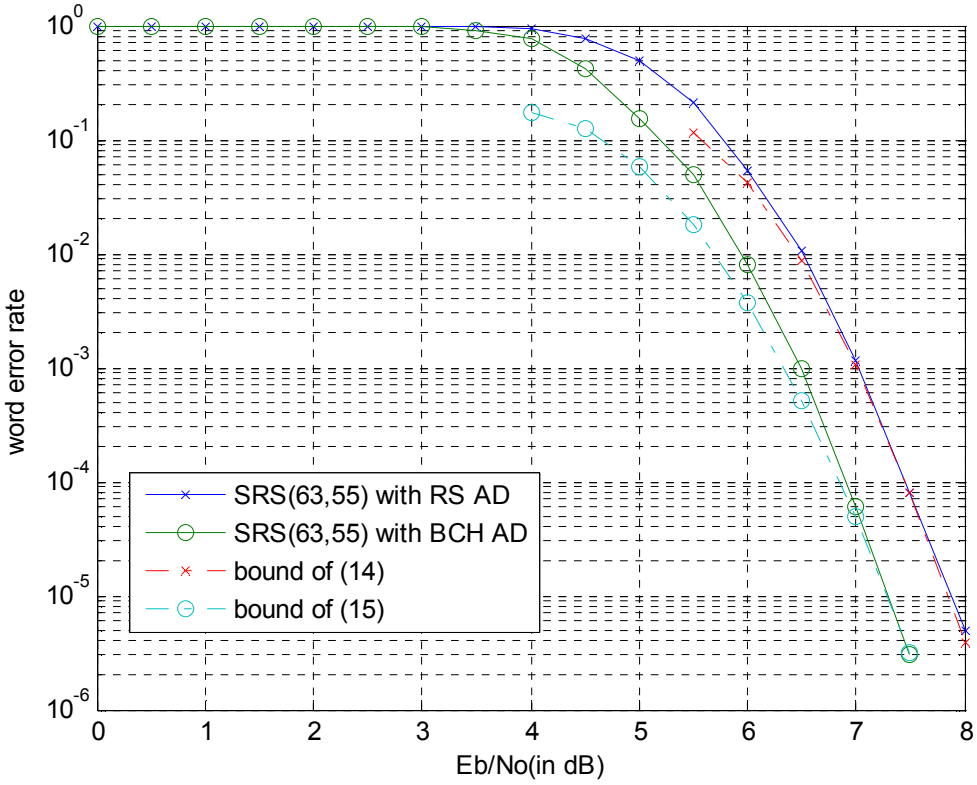


Figure 2: The error performance of RS and BCH algebraic decoding for a shortened (63, 55) RS code with BPSK coherent system over AWGN channels

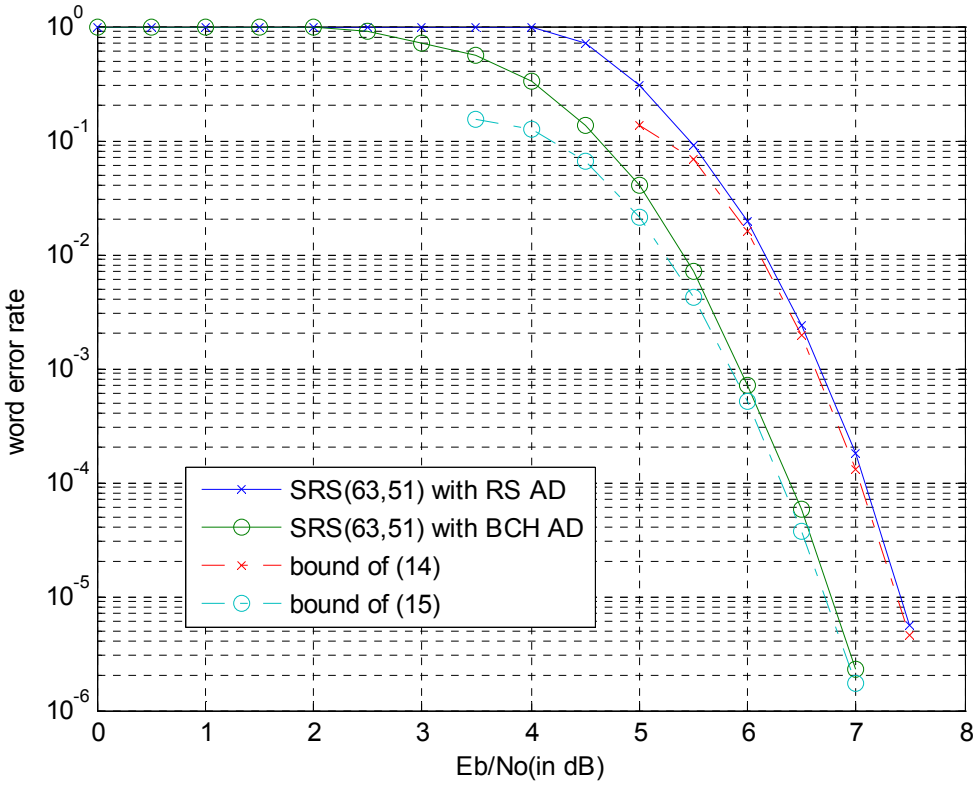


Figure 3: The error performance of RS and BCH algebraic decoding for a shortened (63, 51) RS code with BPSK coherent system over AWGN channels

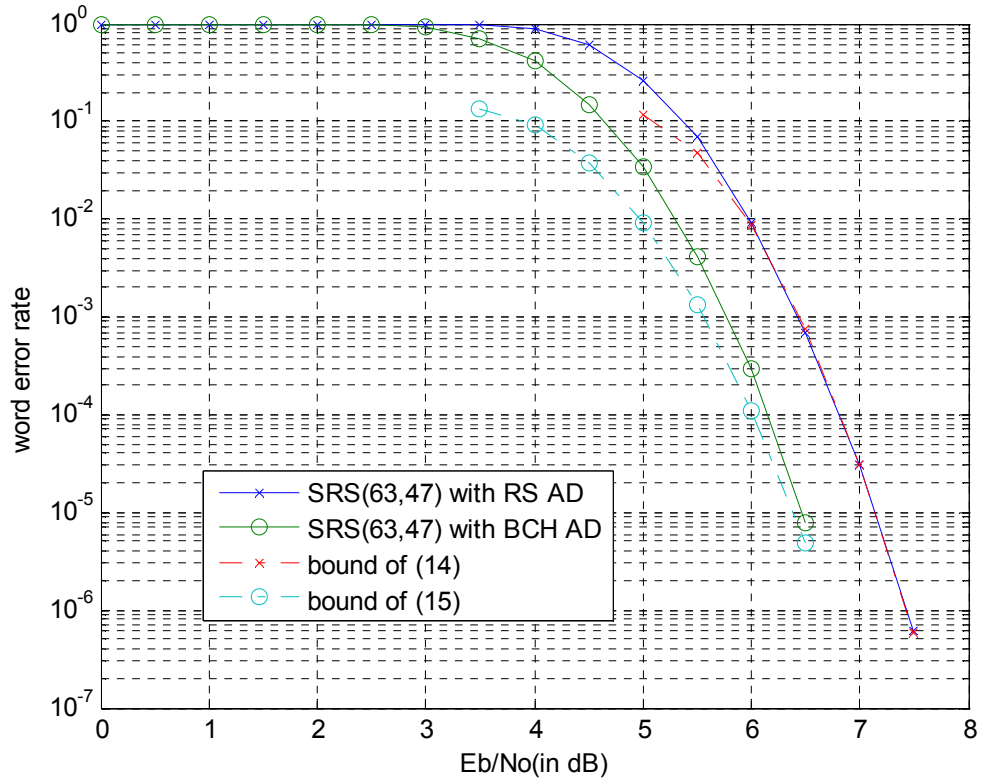


Figure 4: The error performance of RS and BCH algebraic decoding for a shortened (63, 47) RS code with BPSK coherent system over AWGN channels

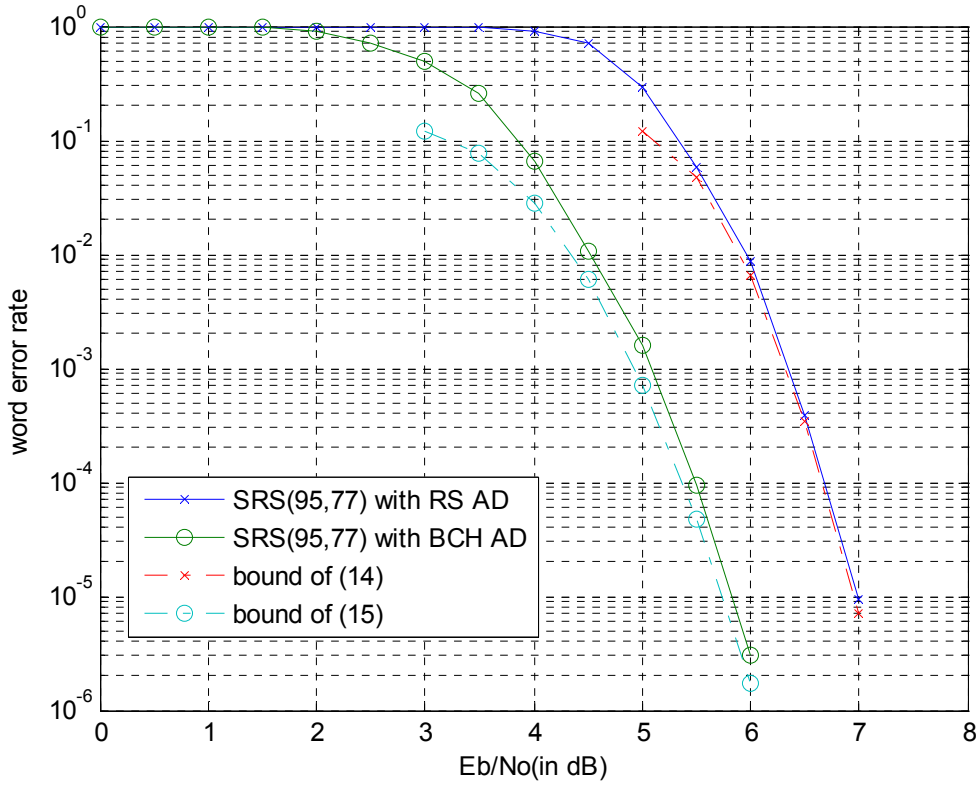


Figure 5: The error performance of RS and BCH algebraic decoding for a shortened (95, 77) RS code with BPSK coherent system over AWGN channels

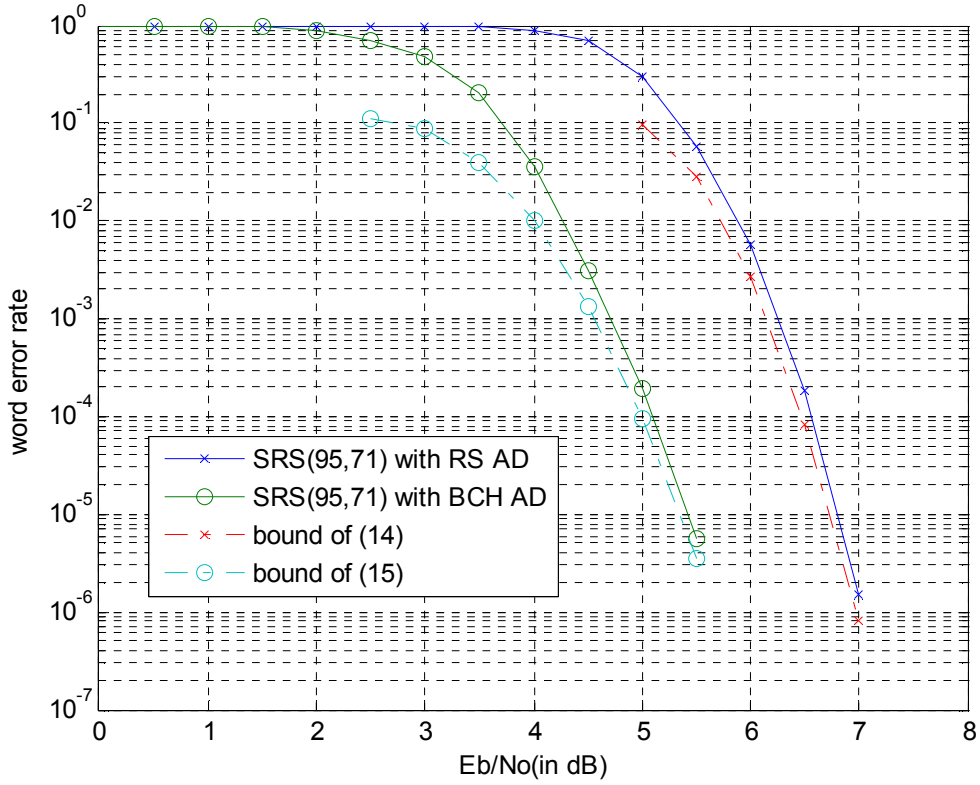


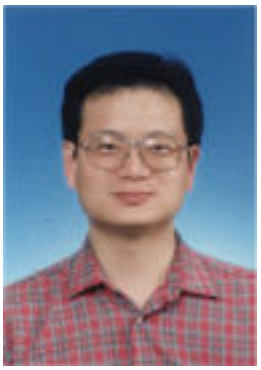
Figure 6: The error performance of RS and BCH algebraic decoding for a shortened (95, 71) RS code with BPSK coherent system over AWGN channels

Table 1: the proposed method for shortening RS codes over $GF(2^8)$

(N, K, t) RS code	(N, k) BCH subcode	L: number of shortened symbols in mother RS code	l: number of deleted BCH subcodes	x: total number of shortened bits in residual BCH subcodes	shortened (N' , K') RS code
(255,253,1)	(255,247)	192	6	6	(63, 61)
(255,251,2)	(255,239)	192	6	6	(63, 59)
(255,249,3)	(255,231)	192	6	6	(63, 57)
(255,247,4)	(255,223)	192	6	6	(63, 55)
(255,245,5)	(255,215)	192	6	6	(63, 53)
(255,243,6)	(255,207)	192	6	6	(63, 51)
(255,241,7)	(255,199)	192	6	6	(63, 49)
(255,239,8)	(255,191)	192	6	6	(63, 47)
(255,237,9)	(255,187)	160	5	5	(95, 77)
(255,235,10)	(255,179)	160	5	5	(95, 75)
(255,233,11),	(255,171)	160	5	5	(95, 73)
(255,231,12)	(255,163)	160	5	5	(95, 71)
(255,229,13)	(255,155)	160	5	5	(95, 69)
(255,227,14),	(255,147)	160	5	5	(95, 67)
(255,225,15)	(255,139)	160	5	5	(95, 65)
(255,223,16)	(255,131)	160	5	5	(95, 63)
(255,221,17)	(255,131)	160	5	5	(95, 61)
(255,219,18)	(255,131)	160	5	5	(95, 59)
(255,217,19)	(255,123)	160	5	5	(95, 57)
(255,215,20)	(255,115)	160	5	5	(95, 55)
(255,213,21)	(255,115)	160	5	5	(95, 53)
(255,211,22)	(255,107)	160	5	5	(95, 51)
(255,209,23)	(255, 99)	160	5	5	(95, 49)
(255,207,24)	(255, 91)	160	5	5	(95, 47)
(255,205,25)	(255, 91)	160	5	5	(95, 45)
(255,203,26)	(255, 87)	160	5	5	(95, 43)
(255,201,27)	(255, 79)	160	5	5	(95, 41)
(255,199,28)	(255, 71)	160	5	5	(95, 39)
(255,197,29)	(255, 71)	160	5	5	(95, 37)
(255,195,30)	(255, 63)	160	5	5	(95, 35)
(255,193,31)	(255, 55)	160	5	5	(95, 33)

Table 1 (Cont.): the proposed way to shortened RS codes over $GF(2^8)$

(N, K, t) RS code	(N, k) BCH subcode	L: number of shortened symbols in mother RS code	l :number of deleted BCH subcodes	x : total number of shortened bits in residual BCH subcodes	shortened (N' , K') RS code
(255,191,32)	(255, 47)	160	5	5	(95, 31)
(255,189,33)	(255, 47)	160	5	5	(95, 29)
(255,187,34)	(255, 47)	160	5	5	(95, 27)
(255,185,35)	(255, 47)	160	5	5	(95, 25)
(255,183,36)	(255, 47)	160	5	5	(95, 23)
(255,181,37)	(255, 47)	160	5	5	(95, 21)
(255,179,38)	(255, 47)	160	5	5	(95, 19)
(255,177,39)	(255, 47)	160	5	5	(95, 17)
(255,175,40)	(255, 47)	128	4	4	(127, 47)
(255,173,41)	(255, 47)	128	4	4	(127, 45)
(255,171,42)	(255, 47)	128	4	4	(127, 43)
(255,169,43)	(255, 45)	128	4	4	(127, 41)
(255,167,44)	(255, 37)	128	4	4	(127, 39)
(255,165,45)	(255, 37)	128	4	4	(127, 37)
(255,163,46)	(255, 29)	128	4	4	(127, 35)
(255,161,47),	(255, 29)	128	4	4	(127, 33)
(255,159,48)	(255, 21)	128	4	4	(127, 31)
(255,157,49)	(255, 21)	128	4	4	(127, 29)
(255,155,50)	(255, 21)	128	4	4	(127, 27)
(255,151,52)	(255, 21)	128	4	4	(127, 23)
(255,149,53)	(255, 21)	128	4	4	(127, 21)
(255,147,54)	(255, 21)	128	4	4	(127, 19)
(255,145,55)	(255, 21)	128	4	4	(127, 17)
(255,143,56)	(255, 13)	128	4	4	(127, 15)
(255,141,57)	(255, 13)	128	4	4	(127, 13)
(255,139,58)	(255, 13)	128	4	4	(127, 11)
(255,137,59)	(255, 13)	128	4	4	(127, 9)
(255,135,60)	(255, 9)	128	4	4	(127, 7)
(255,133,61)	(255, 9)	128	4	4	(127, 5)
(255,131,62)	(255, 9)	96	3	3	(159, 35)
(255,129,63)	(255, 9)	96	3	3	(159, 33)



Ta-Hsiang Hu received the B.S.E.E. degree from Chung Cheng Institute of Technology, Tao-Yuan, Taiwan, in 1984, the M.S.E.E. degree from Naval Postgraduate School, Monterey, CA, in 1991, and the Ph.D. degree in electrical engineering from University of Hawaii at Manoa, Honolulu, in 2001. From 1991 to 2004, he had been on the faculty of the Department of Electrical Engineering, Chung Cheng Institute of Technology, National Defense University, Tao-Yuan, Taiwan. In 2004, he joined the faculty of the Department of Electrical Engineering, Dayeh University, Changhua, Taiwan. His current research interests include coding theory, wireless communications, and VLSI design.

Ming-Hua Chang received the B.S. degree in the Electrical Engineering from Chinese Culture University, Taipei, Taiwan, in 1990, the M.S. degree in the Electrical Engineering from Chung Hua University, Hsinchu, Taiwan, in 1996, and the Ph.D. degree in the Electrical Engineering from School of Defense Science, Chung Cheng Institute of Technology, National Defense University, Taoyuan, Taiwan, in 2008. From1998 to 2009, he has been on the faculty of the Department of Electronic Engineering, Chin Min Institute of Technology. In 2009, he joined the faculty of the Department of Electronic Engineering, Jinwen University of Science and Technology. Currently he is an associate professor. His current research interests include error control coding, wireless communications.