General Disclaimer

One or more of the Following Statements may affect this Document

- This document has been reproduced from the best copy furnished by the organizational source. It is being released in the interest of making available as much information as possible.

- This document may contain data, which exceeds the sheet parameters. It was furnished in this condition by the organizational source and is the best copy available.

- This document may contain tone-on-tone or color graphs, charts and/or pictures, which have been reproduced in black and white.

- This document is paginated as submitted by the original source.

- Portions of this document are not fully legible due to the historical nature of some of the material. However, it is the best reproduction available from the original submission.

FAST DECODING OF A d_{min} = 6 RS CODE

by

Huijie Deng
Department of Electrical Engineering
Illinois Institute of Technology
Chicago, IL 60616

Daniel J. Costello, Jr.*
Department of Electrical Engineering
University of Notre Dame
Notre Dame, IN 46556

December, 1983

This work was supported by NASA under Grant NAG 2-202.

---

* On leave from the Illinois Institute of Technology

There are several known approaches to decoding RS codes. One approach is the iterative algorithm [1], [2]. It has the advantage of easy implementation, but does not meet the high-speed requirement, since the decoding time is too long. Another approach is the table-lookup method [1], by which high-speed decoding is achievable. The drawback is that even for moderate code length r, the implementation of this decoding scheme becomes inpractical, since either a large storage or complicated logic circuitry is needed. For example, if the (37,32) d_{min}=6 RS code over GF(2^8) is used to correct any two or fewer byte errors and detect any three byte errors, the decoding table would contain $(2^8-1)\ \binom{37}{1} + (2^8-1)^2\ \binom{37}{2} \approx 4.3 \times 10^7$ correctable error patterns!

In this report, we present a method for decoding a $d_{min} = 6$ RS code. The method satisfies both high-speed and easy implementation requirements.

I. The $d_{min} = 6$ RS Code and it's Properties

In this section we specify the two-byte-error-correcting and three-byte-error-detecting RS code and show some of it's properties.

The generator polynomial for the $d_{min} = 6$ RS code is given by

$$g(x) = \prod_{i=-2}^{2} (x + \alpha^i), \tag{1}$$

where we choose α to be a primitive element of GF(2^m). The parity-check matrix, $\underline{H}$, of the code specified by Eq. (1) can be written as

$$\underline{H} = \begin{bmatrix} 1 & \alpha^{-2} & (\alpha^{-2})^2 & \cdots & (\alpha^{-2})^{n-1} \\ 1 & \alpha^{-1} & (\alpha^{-1})^2 & \cdots & (\alpha^{-1})^{n-1} \\ 1 & 1 & 1 & \cdots & 1 \\ 1 & \alpha & (\alpha)^2 & \cdots & (\alpha)^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \end{bmatrix} \tag{2}$$

where $n \leq 2^m - 1$ and $1 = \alpha^0$ is the identity element of $GF(2^m)$. Because the code has $d_{min} = 6$, then every combination of $d_{min} - 1 = 5$ or fewer columns of $\underline{H}$ is linearly independent, and the code is capable of correcting any two or fewer byte errors and simultaneously detecting any combination of three byte errors [1].

Let $\underline{V} = (v_0, v_1, \ldots, v_{n-1})$ be a code word that is transmitted over a noisy channel. Let $\underline{\gamma} = (\gamma_0, \gamma_1, \ldots, \gamma_{n-1})$ be the received vector at the output of the channel. Because of the channel noise, $\underline{\gamma}$ may be different from $\underline{V}$. The vector sum

$$\underline{e} = \underline{\gamma} + \underline{V} = (e_0, e_1, \ldots, e_{n-1}) \tag{3}$$

is an n-tuple where $e_i \neq 0$ for $\gamma_i \neq v_i$ and $e_i = 0$ for $\gamma_i = v_i$. This n-tuple is called the error pattern. When $\underline{\gamma}$ is received, the decoder computes the syndrome $\underline{S}$,

$$\begin{aligned} \underline{S}^T &= \underline{\gamma}\,\underline{H}^T = (\underline{v} + \underline{e})\underline{H}^T = \underline{e}\,\underline{H}^T \\ &= (S_{-2}, S_{-1}, S_0, S_1, S_2) \end{aligned} \tag{4}$$

Since $\underline{V}\,\underline{H}^T = \underline{0}$, the syndrome $\underline{S}$ computed from the received $\underline{\gamma}$ depends only on the error pattern $\underline{e}$, and not on the transmitted code word $\underline{V}$ [1].

Let $\underline{S}_S$, $\underline{S}_d$, and $\underline{S}_T$ deonte the syndromes corresponding to single, double and triple byte error patterns, respectively. Then from Eq. (4) we have,

$$\underline{S}_S = \begin{bmatrix} e\alpha^{-2i} \\ e\alpha^{-i} \\ e \\ e\alpha^{i} \\ e\alpha^{2i} \end{bmatrix} \tag{5}$$

where e is the error value and i is the error location.

$$\underline{S}_d = \begin{bmatrix} e_1\alpha^{-2i} + e_2\alpha^{-2j} \\ e_1\alpha^{-i} + e_2\alpha^{-j} \\ e_1 + e_2 \\ e_1\alpha^{i} + e_2\alpha^{j} \\ e_1\alpha^{2i} + e_2\alpha^{2j} \end{bmatrix} \tag{6}$$

where $0 \leq i < j \leq 2^m - 1$

and

$$\underline{S}_T = \begin{bmatrix} e_1\alpha^{-2i} + e_2\alpha^{-2j} + e_3\alpha^{-2k} \\ e_1\alpha^{-1} + e_2\alpha^{-j} + e_3\alpha^{-k} \\ e_1 + e_2 + e_3 \\ e_1\alpha^{i} + e_2\alpha^{j} + e_3\alpha^{k} \\ e_1\alpha^{2i} + e_2\alpha^{2j} + e_3\alpha 2k \end{bmatrix} \tag{7}$$

where $0 \leq i < j < k \leq 2^m - 1$.

Before proceeding, we need to prove some properties of the code which will be used later.

Property 1

$$\underline{S}_S \neq \underline{S}_d \neq \underline{S}_T \tag{8}$$

holds true for any single, double, and triple byte error patterns.

Proof:

First we show that . $\neq \underline{S}_d$. If not, then there exists at least one single byte error pattern and one double byte error pattern such that

$$\underline{S}_S = \underline{S}_d$$

or

$$\underline{S}_S + \underline{S}_d = 0.$$

From Eqs. (5) and (6) we have

$$\begin{bmatrix} e_1\alpha^{-2i_1} \\ e_1\alpha^{-i_1} \\ e_1 \\ e_1\alpha^{i_1} \\ e_1\alpha^{2i_1} \end{bmatrix} + \begin{bmatrix} e_2\alpha^{-2i_2} + e_3\alpha^{-2i_3} \\ e_2\alpha^{-i_2} + e_3\alpha^{-i_3} \\ e_2 + e_3 \\ e_2\alpha^{i_2} + e_3\alpha^{i_3} \\ e_2\alpha^{2i_2} + e_3\alpha^{2i_3} \end{bmatrix}$$

$$= e_1 \begin{bmatrix} \alpha^{-2i_1} \\ \alpha^{-i_1} \\ 1 \\ \alpha^{i_1} \\ \alpha^{2i_1} \end{bmatrix} + e_2 \begin{bmatrix} \alpha^{-2i_2} \\ \alpha^{-i_2} \\ 1 \\ \alpha^{i_2} \\ \alpha^{2i_2} \end{bmatrix} + e_3 \begin{bmatrix} \alpha^{-2i_3} \\ \alpha^{-i_3} \\ 1 \\ \alpha^{i_3} \\ \alpha^{2i_3} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \qquad \text{for } i_2 < i_3.$$

This contradicts the fact that any 5 or fewer columns of $\underline{H}$ in Eq. (2) are linearly independent! Hence $\underline{S}_s \neq \underline{S}_d$. By the same argument we can prove that the other cases also hold true. Q.E.D.

Lemma 1

If α is a primitive element of $GF(2^m)$, then

$$\alpha^{-i} + \alpha^{-j} \neq 0 \qquad (9.1)$$

$$\alpha^{-2i} + \alpha^{-2j} \neq 0 \qquad (9.2)$$

for $0 \leq i < j \leq 2^m - 1$.

Proof:

If $\alpha^{-i} + \alpha^{-j} = 0$, multiply both sides by $\alpha^{i+j} \neq 0$. Then we have $\alpha^{i} + \alpha^{j} = 0$, but this is impossible since α is a primitive element. Similarly we can show Eq. (9.2) is also correct. Q.E.D.

Let $\underline{S}_d = (S_{-2}, S_{-1}, S_0, S_1, S_2)^T$. From Eq. (6) we have the following equations:

$$S_{-2} = e_1 \alpha^{-2i} + e_2\alpha^{-2j} \qquad (10.1)$$

$$S_{-1} = e_1\alpha^{-i} + e_2\alpha^{-j} \qquad (10.2)$$

$$S_0 = e_1 + e_2 \qquad (10.3)$$

$$S_1 = e_1\alpha^{i} + e_2\alpha^{j} \qquad (10.4)$$

$$S_2 = e_1\alpha^{2i} + e_2\alpha^{2j} \qquad (10.5)$$

Property 2

Let $\underline{S}_d = (S_{-2}, S_{-1}, S_0, S_1, S_2)^T$ be the syndrome corresponding to a double byte error pattern with error values e_1 and e_2 at locations i and j, respectively. Let N denote the number of zero elements of $\underline{S}_d$. Then,

$N \leq 2$,

and the only two cases for which the equal sign can hold for some values of i and j are

1) $S_{-1} = S_2 = 0$

2) $S_1 = S_{-2} = 0$

Proof:

It can easily be seen from Lemma 1 that the following vectors

$(1,1)$, (α^i,α^j), $(\alpha^{2i},\alpha^{2j})$, $(\alpha^{-i},\alpha^{-j})$, and $(\alpha^{-2i},\alpha^{-2j})$,

where $0 \leq i < j \leq 2^m - 1$, are pairwise linearly independent except for the two pairs:

1) $(\alpha^{-i},\alpha^{-j})$, $(\alpha^{2i},\alpha^{2j})$, 2) (α^i,α^j), $(\alpha^{-2i},\alpha^{-2j})$.

These two pairs can be linearly dependent for some values of i and j.

Combining this fact with Eqs. (10.1) - (10.5), we obtain the property.

Q.E.D.

Property 3

Let $\underline{S}_d = (S_{-2}, S_{-1}, S_0, S_1, S_2)^T$. Then the equations

$$S_1S_{-2} + S_{-1}S_0 \neq 0 \qquad (11.1)$$

$$S_0S_1 + S_2S_{-1} \neq 0 \qquad (11.2)$$

$$S_2S_{-2} + S_0^2 \neq 0 \qquad (11.3)$$

hold true for any double byte error pattern.

Proof:

1) Suppose $S_2S_{-2} + S_0^2 = 0$. From Eqs. (10.1), (10.3) and (10.5) we obtain

$$(e_1\alpha^{2i} + e_2\alpha^{2j})\,(e_1\alpha^{-2i} + e_2\alpha^{-2j}) + (e_1 + e_2)^2 = 0.$$

Expanding this equation and performing some simplification gives us

$$\alpha^{2i-2j} + \alpha^{-2i+2j} = 0.$$

But this is impossible since α is a primitive element and $i \neq j$.

Therefore, $S_2S_{-2} + S_0^2 \neq 0$.

2) Suppose $S_1S_{-2} + S_{-1}S_0 = 0$, that is $S_1S_{-2} = S_{-1}S_0$.

From Eqs. (10.1) - (10.4) we have

$$(e_1\alpha^{i} + e_2\alpha^{j})\,(e_1\alpha^{-2i} + e_2\alpha^{-2j}) = (e_1\alpha^{-i} + e_2\alpha^{-j})\,(e_1 + e_2).$$

After some simplification we obtain

$$\alpha^{i-2j} + \alpha^{j-2i} = \alpha^{-i} + \alpha^{-j}.$$

Multiplying both sides by $\alpha^{2i+2j} \neq 0$, the above equation becomes

$$\alpha^{3i} + \alpha^{3j} = \alpha^{i+2j} + \alpha^{j+2i} \qquad (12)$$

or

$$(\alpha^i + \alpha^j)\,(\alpha^{2i} + \alpha^{i+j} + \alpha^{2j}) = \alpha^{i+j}\,(\alpha^i + \alpha^j).$$

This can be reduced to

$$\alpha^{2i} + \alpha^{2j} = 0 \qquad \text{for } i \neq j.$$

But this is impossible. Hence $S_1S_{-2} + S_{-1}S_0 \neq 0$.

3) Suppose $S_0S_1 + S_2S_{-1} = 0$. In the same way as above we obtain

$$\alpha^{3i} + \alpha^{3j} = \alpha^{i+2j} + \alpha^{j+2i}.$$

This is exactly the same as Eq. (12). Hence the equality is invalid, and $S_0S_1 + S_2S_{-1} \neq 0$. O.E.D.

II. Decoding Using The Quadratic Equation

In this section we show that the well known quadratic equation over $GF(2^m)$ can be used to decode the code described in Section I. Also we present a method of solving it.

It was shown in Lemma 1 that if α is a primitive element of $GF(2^m)$, then $\alpha^{-i} + \alpha^{-j} \neq 0$ and $\alpha^{-2i} + \alpha^{-2j} \neq 0$ both hold true for any $0 \leq i < j \leq 2^m - 1$. From Eqs. (10.1) and (10.3) we have

$$e_1 = \frac{\det \begin{vmatrix} S_0 & 1 \\ S_{-2} & \alpha^{-2j} \end{vmatrix}}{\det \begin{vmatrix} 1 & 1 \\ \alpha^{-2i} & \alpha^{-2j} \end{vmatrix}} = \frac{S_{-2} + S_0\,\alpha^{-2j}}{(\alpha^{-i} + \alpha^{-j})^2} \tag{13}$$

From Eqs. (10.2) and (10.3) we have

$$e_1 = \frac{\det \begin{vmatrix} S_0 & 1 \\ S_{-1} & \alpha^{-j} \end{vmatrix}}{\det \begin{vmatrix} 1 & 1 \\ \alpha^{-i} & \alpha^{-j} \end{vmatrix}} = \frac{S_{-1} + S_0\,\alpha^{-j}}{\alpha^{-i} + \alpha^{-j}} \tag{14}$$

Then

$$\frac{S_{-1} + S_0\,\alpha^{-j}}{\alpha^{-i} + \alpha^{-j}} = \frac{S_{-2} + S_0\,\alpha^{-2j}}{(\alpha^{-i} + \alpha^{-j})^2}\ . \tag{15}$$

Now multiply both sides by $(\alpha^{-i} + \alpha^{-j})^2 \neq 0$. Eq. (15) becomes

$$(\alpha^{-i} + \alpha^{-j})\,(S_{-1} + S_0\,\alpha^{-j}) = S_{-2} + S_0\,\alpha^{-2j}. \tag{16}$$

After simplification we have

$$S_{-1}(\alpha^{-i} + \alpha^{-j}) + S_{-2} + S_0\,\alpha^{-i-j} = 0. \tag{17}$$

Multiplying (17) by α^{i+j} gives us

$$S_{-1}(\alpha^{i} + \alpha^{j}) + S_{-2}\,\alpha^{i}\,\alpha^{j} + S_0 = 0. \tag{18}$$

In the same way, from Eqs. (10.3) - (10.5), we can obtain

$$S_1(\alpha^{i} + \alpha^{j}) + S_0\,\alpha^{i}\,\alpha^{j} + S_2 = 0. \tag{19}$$

Now define

$$b \overset{\Delta}{=} \alpha^{i} + \alpha^{j} \tag{20.1}$$

$$c \overset{\Delta}{=} \alpha^{i}\,\alpha^{j}. \tag{20.2}$$

Eqs. (18) and (19) can be written as

$$S_{-1}b + S_{-2}c + S_0 = 0 \tag{21.1}$$

$$S_1 b + S_0 c + S_2 = 0. \tag{21.2}$$

Also define

$$\gamma_1 \overset{\Delta}{=} S_1 S_{-2} + S_{-1}\,S_0 \tag{22.1}$$

$$\gamma_2 \overset{\Delta}{=} S_2 S_{-2} + S_0^{2} \tag{22.2}$$

$$\gamma_3 \overset{\Delta}{=} S_0 S_1 + S_2 S_{-1}. \tag{22.3}$$

Solving Eqs. (21.1), (21.2) for b and c, we have

$$b = \frac{\gamma_2}{\gamma_1} = \alpha^{i} + \alpha^{j} \tag{23.1}$$

$$c = \frac{\gamma_3}{\gamma_1} = \alpha^{i}\alpha^{j} \tag{23.2}$$

for $\gamma_1 \neq 0$. Also, from Eqs. (20.1) and (20.2) we see that α^{i} and α^{j} are the roots of

$$y^2 + by + c = 0. \tag{24}$$

This is the well-known quadratic equation over $GF(2^m)$. We will see in Section III that Eq. (24) plays an important role in decoding. Therefore we call it the "decoding equation". Because of it's importance, in the remainder of this section we discuss a method of solving it.

The formula for the roots of the quadratic equation $y^2 + by + c = 0$ is $(-b \pm \sqrt{b^2 - 4c})/2$. Unfortunately, for finite fields of characteristic two, this formula is not applicable because the denominator is zero ($2 = 1+1 = 0$). However, there are several known approaches to solving this problem. One way of finding the roots is by trying each element of the field in sequence [3]. But this is unacceptable for fast decoding because it takes a long time. The method given in [4] is probably the best one known. We present it here.

Let

$$y = bx. \tag{25}$$

Then Eq. (24) becomes

$$x^2 + x + K = 0, \tag{26}$$

where $K = c/b^2$.

Let β be an element of $GF(2^m)$, and define

$$T_2(\beta) = \sum_{i=0}^{m-1} \beta^{2^i}. \tag{27}$$

$T_2(\beta)$ is called the trace of β. It is either zero or one [4]. For even m, define

$$T_4(\beta) = \sum_{i=0}^{(m-2)/2} \beta^{2^{2i}}. \tag{28}$$

If (26) has solutions, then $T_4(\beta)$ is either zero or one [4]. Eq. (26) has solutions in $GF(2^m)$ if and only if $T_2(K) = 0$, where $K = c/b^2$ [2], [5].

Let x_1 be a solution of Eq. (26), then $x_2 = 1 + x_1$ is the other solution. Suppose $T_2(K) = 0$, i.e., Eq. (26) has solutions. Then we have the following results [4]:

1) m odd.

$$x_1 = \sum_{j \in J} K^{2^j} = \sum_{i \in I} K^{2^i} \tag{29}$$

where $I = \{1,3,5,\ldots,m-2\}$, $J = \{0,2,4,\ldots,m-1\}$.

2) $m \equiv 2$ modulo 4

$$x_1 = \sum_{i=0}^{(m-6)/4} (K + K^2)^{2^{2+4i}}, \quad \text{for } T_4(K) = 0, \tag{30.1}$$

$$x_1 = \alpha_1 + \sum_{i=0}^{(m-6)/4} (K + K^2)^{2^{2+4i}}, \quad \text{for } T_4(K) = 1, \tag{30.2}$$

where α_1 is a solution of the equation $\alpha_1^2 + \alpha_1 + 1 = 0$.

3) $m \equiv 0$ modulo 4.

$$x_1 = S + S^2 + K^{2^{m-1}} \left(1 + \sum_{i=0}^{(m/4)-1} K^{2^{2i+m/2}}\right), \text{ for } T_4(K) = 1, \tag{31}$$

where $S = \sum_{j=1}^{(m/4)-1} \sum_{i=j}^{(m/4)-1} K^{(2^{2i-1+m/2} + 2^{2j-2})}$.

For $T_4(K) = 0$, select an element β of $GF(2^m)$ such that $T_2(\beta) = 1$, compute $K_1 = \beta + \beta^2$, and solve $z^2 + z + K_1 + K = 0$ using Eq. (31) with K replaced by $K_1 + K$. Then $x_1 = \beta + z_1$ is a solution of Eq. (26), where z_1 is obtained from (31). For $m = 4,8,12$, Eq. (31) reduces to the following forms:

$m = 4$, $x_1 = K^8 + K^{12}$;

$m = 8$, $x_1 = K^{33} + K^{66} + K^{129} + K^{132}$;

$m = 12$, $x_1 = K^{2048}(1 + K^{64} + K^{256} + K^{1024}) + K^{129} + K^{258} + K^{506} + K^{513} + K^{1026} + K^{1032}$.

III. Decoding of the Code

In this section we describe the decoding scheme for the double-byte-error-correcting and triple-byte-error-detecting RS code specified by Eqs. (1) and (2), through an analysis of the decoding equation (24) obtained in Section II. For convenience, we rewrite Eq. (24) as

$$y^2 + by + c = 0 \tag{32.1}$$

where

$$b = \alpha^i + \alpha^j = \frac{\gamma_2}{\gamma_1} = \frac{S_2S_{-2} + S_0^2}{S_1S_{-2} + S_{-1}S_0} \tag{32.2}$$

$$c = \alpha^i\alpha^j = \frac{\gamma_3}{\gamma_1} = \frac{S_0S_1 + S_2S_{-1}}{S_1S_{-2} + S_{-1}S_0}. \tag{32.3}$$

Now suppose that a double byte error pattern with error values e_1 and e_2 at locations i and j (i<j) occurs. By our definition, $\underline{S}_d = (S_{-2}, S_{-1}, S_0, S_1, S_2)^T$ is the syndrome associated with this error pattern. From property 3 in Section I we know that $\gamma_1 = S_1S_{-2} + S_{-1}S_0 \neq 0$, $\gamma_2 = S_2S_{-2} + S_0^2 \neq 0$, and $\gamma_3 = S_0S_1 + S_2S_{-1} \neq 0$. Therefore b and c in Eqs. (32.2) and (32.3) exist. By definition $b = \alpha^i + \alpha^j$ and $c = \alpha^i\alpha^j$ for $0 \leq i < j \leq 2^m - 1$. Hence Eq. (32.1) has two roots, α^i and α^j. Thus we obtain:

Theorem 1: If S_{-2}, S_{-1}, S_0, S_1, S_2 are the elements of $\underline{S}_d$, decoding equation (32.1) has two roots, α^i and α^j, where i and j are the two error byte locations and $0 \leq i < j \leq 2^m-1$.

In other words, whenever a double byte error occurs, it's error locations can be found by solving the decoding equation (32.1).

Since $\alpha^i + \alpha^j \neq 0$ when α is a primitive element of $GF(2^m)$, Eqs. (10.3), (10.4) and (32.2) imply that

$$e_1 = \frac{\det\begin{vmatrix} S_0 & 1 \\ S_1 & \alpha^j \end{vmatrix}}{\det\begin{vmatrix} 1 & 1 \\ \alpha^i & \alpha^j \end{vmatrix}} = \frac{S_0\alpha^j + S_1}{\alpha^i + \alpha^j} = \frac{S_0\alpha^j + S_1}{b} \tag{33.1}$$

and

$$e_2 = S_0 + e_1, \tag{33.2}$$

where e_1 and e_2 are the error values at locations i and j of the double byte error pattern.

Now let $\underline{S}_3 = (S_{-2}, S_{-1}, S_0, S_1, S_2)^T$ be the syndrome corresponding to a single byte error pattern with error value e at location i. From Eq. (5) we have:

$$S_{-2} = e\,\alpha^{-2i} \tag{34.1}$$

$$S_{-1} = e\,\alpha^{-i} \tag{34.2}$$

$$S_0 = e \tag{34.3}$$

$$S_1 = e\,\alpha^{i} \tag{34.4}$$

$$S_2 = e\,\alpha^{2i} \tag{34.5}$$

From Eqs. (34.1) - (34.5), we see that

$$\frac{S_{-1}}{S_{-2}} = \frac{S_0}{S_{-1}} = \frac{S_1}{S_0} = \frac{S_2}{S_1} = \alpha^i. \tag{35}$$

Eq. (35) is equivalent to

$$\gamma_1 = S_1S_{-2} + S_{-1}S_0 = 0 \tag{36.1}$$

$$\gamma_2 = S_2S_{-2} + S_0^2 = 0 \tag{36.2}$$

$$\gamma_3 = S_0S_1 + S_2S_{-1} = 0. \tag{36.3}$$

The above result implies the following theorem:

Theorem 2:

If S_{-2}, S_{-1}, S_0, S_1, S_2 are the elements of $\underline{S}_3$, then $\gamma_1 = \gamma_2 = \gamma_3 = 0$.

In other words, whenever a single byte error occurs, $\gamma_1 = \gamma_2 = \gamma_3 = 0$.

From Eqs. (34.3) and (34.4) we have

$$\alpha^i = \frac{S_1}{S_0} \tag{37.1}$$

$$e = S_0, \tag{37.2}$$

where i gives the error location and e is the error value of the single byte error pattern.

From properties 1-3 in Section I and Theorems 1 and 2, we have:

Theorem 3:

If more than two elements of the syndrome $\underline{S} = (S_{-2}, S_{-1}, S_0, S_1, S_2)^T$ equal zero; or if γ_1, γ_2, and γ_3 are not all equal to zero, but at least one of them does equal zero; or if the decoding equation (32.1) does not have roots in $GF(2^m)$, then at least three byte errors have occurred.

We now summarize the decoding scheme obtained above for the double-byte-error-correcting and triple-byte-error-detecting Reed-Solomon Code defined by Eqs. (1) and (2). Receive $\underline{\gamma}$, and calculate the syndrome $\underline{S}^T = \underline{\gamma}\underline{H}^T = (S_{-2}, S_{-1}, S_0, S_1, S_2)$.

1) If $\underline{S} = \underline{0}$, decide that no errors occurred.
2) If more than two elements of the syndrome equal zero, decide that at least 3 errors occurred.
3) Compute γ_1, γ_2, γ_3. If $\gamma_1 = \gamma_2 = \gamma_3 = 0$, calculate $\alpha^i = \frac{S_1}{S_0}$, and correct a single byte error with error value $e = S_0$ at location i.
4) If γ_1, γ_2, γ_3 are not all zero but at least one of them equals zero, decide that at least three byte errors occurred.
5) If $\gamma_1 \neq 0$, $\gamma_2 \neq 0$, $\gamma_3 \neq 0$, compute $K = c/b^2$ and $T_2(K)$. If $T_2(K) = 1$, decide that at least three byte errors occurred.
6) If $T_2(K) = 0$, solve the decoding equation (32.1) and find the roots α^i and α^j. Compute $e_1 = (S_0\alpha^j + S_1)/b$, $e_2 = S_0 + e_1$, and correct a double byte error with error values e_1, e_2 at locations i and j, respectively.

IV. Decoding of the Extended Code

The parity-check matrix $\underline{H}$ given in (2) can be extended to form a new parity-check matrix given by

$$\underline{H}_1 = \begin{bmatrix} & 1 & 0 \\ & 0 & 0 \\ \underline{H} & 0 & 0 \\ & 0 & 0 \\ & 0 & 1 \end{bmatrix} \tag{38}$$

The code C_1 specified by $\underline{H}_1$ is an $(n+2, n-3)$ $d_{min} = 6$ code, called the extended Reed-Soloman code, where $n \leq 2^m - 1$. [6,7,8].

In the same way as in Section I we can show that

$$\underline{S}_S \neq \underline{S}_d \neq \underline{S}_T \tag{39}$$

holds true for all single, double, and triple byte error patterns. And obviously if the error locations are confined to locations 0 through n-1, all the previous results apply.

Now assume that errors occur at locations n and/or n+1. Then the syndrome for the single byte error pattern is given by

$$\underline{S}_S = \begin{bmatrix} e \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} S_{-2} \\ S_{-1} \\ S_0 \\ S_1 \\ S_2 \end{bmatrix} \tag{40.1}$$

with an error at location n, or

$$\underline{S}_S = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ e \end{bmatrix} = \begin{bmatrix} S_{-2} \\ S_{-1} \\ S_0 \\ S_1 \\ S_2 \end{bmatrix} \tag{40.2}$$

with an error at location n + 1. For a double byte error pattern, the syndrome is given by

$$\underline{S}_d = \begin{bmatrix} e_1\alpha^{-2i} + e_2 \\ e_1\alpha^{-i} \\ e_1 \\ e_1\alpha^{i} \\ e_1\alpha^{2i} \end{bmatrix} = \begin{bmatrix} S_{-2} \\ S_{-1} \\ S_0 \\ S_1 \\ S_2 \end{bmatrix} \tag{41.1}$$

with two errors at locations i and n, respectively, where $0 \leq i \leq n-1$, and

$$\underline{S}_d = \begin{bmatrix} e_1\alpha^{-2i} \\ e_1\alpha^{-i} \\ e_1 \\ e_1\alpha^{i} \\ e_1\alpha^{2i} + e_2 \end{bmatrix} = \begin{bmatrix} S_{-2} \\ S_{-1} \\ S_0 \\ S_1 \\ S_2 \end{bmatrix} \tag{41.2}$$

with two errors at locations i and n+1, respectively, where $0 \leq i \leq n-1$.

Finally

$$\underline{S}_S = \begin{bmatrix} e_1 \\ 0 \\ 0 \\ 0 \\ e_2 \end{bmatrix} = \begin{bmatrix} S_{-2} \\ S_{-1} \\ S_0 \\ S_1 \\ S_2 \end{bmatrix} \tag{41.3}$$

with two errors at locations n and n+1, respectively.

From (40.1) - (41.3) we obtain the following results. From the received vector $\underline{r}$, compute the syndrome $\underline{S}^T = \underline{r}\,\underline{H}_1^T = (S_{-2}, S_{-1}, S_0, S_1, S_2)$.

1) If

$$S_{-2} \neq S_{-1} = S_0 = S_1 = S_2 = 0, \tag{42}$$

then decide that a single byte error pattern occurred. From (40.1) we have the error value $e = S_{-2}$, and the error location is n.

2) If

$$S_2 \neq S_{-2} = S_{-1} = S_0 = S_1 = 0, \tag{43}$$

then a single byte error pattern has occurred with error value $e = S_2$ at location n+1.

3) If

$$\frac{S_{-1}}{S_{-2}} \neq \frac{S_0}{S_{-1}} = \frac{S_1}{S_0} = \frac{S_2}{S_1}, \tag{44}$$

then decide that a double byte error pattern occurred. From (41.1) we see that the error value $e_1 = S_0$ and $\frac{S_1}{S_0} = \alpha^i$, where i gives the location of e_1. Since $e_2 = S_{-2} + e_1\alpha^{-2i} = S_{-2} + S_0\alpha^{-2i}$, it occurs at location n.

4) If

$$\frac{S_{-1}}{S_{-2}} = \frac{S_0}{S_{-1}} = \frac{S_1}{S_0} \neq \frac{S_2}{S_1} \tag{45}$$

then a double byte error pattern occurs with error values $e_1 = S_0$ and $e_2 = S_2 + S_0\alpha^{2i}$ at locations i and n+1, respectively, where i is obtained from $\alpha^i = \frac{S_1}{S_0}$.

5) If

$$S_{-2} \neq 0,\ S_2 \neq 0, \text{ and } S_{-1} = S_0 = S_1 = 0 \tag{46}$$

then a double byte error pattern occurs with error values $e_1 = S_{-2}$ and $e_2 = S_2$ at locations n and n+1, respectively.

Now we combine the discussion in this section with that of Sections I-III to obtain the following decoding scheme for the double-byte-error-correcting and triple-byte-error-detecting extended Reed-Solomon Code C_1 defined by (38). From the received vector $\underline{r}$, compute the syndrome $\underline{S}^T = \underline{r}\,\underline{H}_1^T = (S_{-2}, S_{-1}, S_0, S_1, S_2)$.

1) If $\underline{S} = \underline{0}$, decide that no errors occurred.

2) If $S_{-2} \neq S_{-1} = S_0 = S_1 = S_2 = 0$, decide that a single byte error pattern occurred with error value $e = S_{-2}$ at location n.

If $S_2 \neq S_{-2} = S_{-1} = S_0 = S_1 = 0$, then a single byte error pattern occurred with error value $e = S_2$ at location n+1.

3) If $\frac{S_{-1}}{S_{-2}} \neq \frac{S_0}{S_{-1}} = \frac{S_1}{S_0} = \frac{S_2}{S_1}$, a double byte error pattern occurred.

$e_1 = S_0$ and $e_2 = S_{-2} + S_0\alpha^{-2i}$ give the error values at locations i and n, respectively, where $\frac{S_1}{S_0} = \alpha^i$.

If $\frac{S_{-1}}{S_{-2}} = \frac{S_0}{S_{-1}} = \frac{S_1}{S_0} \neq \frac{S_2}{S_1}$, a double byte error pattern occurred.

$e_1 = S_0$ and $e_2 = S_2 + S_0\alpha^{2i}$ give the error values at locations i and n+1, respectively, where $\frac{S_1}{S_0} = \alpha^i$.

If $S_{-2} \neq 0$, $S_2 \neq 0$, and $S_{-1} = S_0 = S_1 = 0$, a double byte error pattern occurred, with error values $e_1 = S_{-2}$ and $e_2 = S_2$ at locations n and n+1, respectively.

4) If more than two elements of the syndrome equal zero, decide that at least 3 errors occurred.

5) Compute γ_1, γ_2, γ_3. If $\gamma_1 = \gamma_2 = \gamma_3 = 0$, calculate $\alpha^i = \frac{S_1}{S_0}$, and correct a single byte error with error value $e = S_0$ at location i.

6) If γ_1, γ_2, γ_3 are not all zero, but at least one of them equals zero, decide that at least three byte errors occurred.

7) If $\gamma_1 \neq 0$, $\gamma_2 \neq 0$, $\gamma_3 \neq 0$, compute $K = c/b^2$ and $T_2(K)$. If $T_2(K) = 1$, decide that at least three byte errors occurred.

8) If $T_2(K) = 0$, solve the decoding equation (32.1) and find the roots α^i and α^j. Compute $e_1 = (S_0\alpha^j + S_1)/b$, $e_2 = S_0 + e_1$, and correct a double byte error with error values e_1 and e_2 at locations i and j, respectively.

References

[1] S. Lin and D.J. Costello, Jr., Error Control Coding: Fundamentals and Applications, Prentice-Hall, New Jersey, 1983.

[2] E.R. Berlekamp, Algebraic Coding Theory, McGraw-Hall, New York, 1968.

[3] R.T. Chien, "Cyclic Decoding Procedures for BCH Code," IEEE Trans. Inform. Theory, IT-10, pp. 357-363, Oct. 1964.

[4] C.L. Chen, "Formulas for the Solutions of Quadratic Equations," IEEE Trans. Inform. Theory, IT-28, pp. 792-794, Sept. 1982.

[5] E.R. Berlekamp, H. Rumsey, and G. Solomon, "On the Solution of Algebraic Equations Over Finite Fields," Inform. Contr., pp. 553-564, Oct. 1967.

[6] T. Kasami, S. Lin, and W.W. Peterson, "Some Results on Weight Distributions of BCH Codes," IEEE Trans. Inf. Theory, IT-12, p. 274, April 1966.

[7] T. Kasami, S. Lin, and W.W. Peterson, "Some Results on Cyclic Codes which are Invariant under the Affine Group," Scientific Report AFCRL-66-662, Air Force Cambridge Research Labs., Bedford, Mass., 1966.

[8] J.K. Wolf, "Adding Two Information Symbols to Certain Nonbinary BCH Codes and Some Applications," Bell Syst. Tech. J., 48, pp. 2405-2424, 1969.