Step-by-step decoding algorithm for Reed–Solomon codes

T.-C.Chen, C.-H.Wei and S.-W.Wei

Abstract: A new step-by-step decoding algorithm for decoding Reed–Solomon codes over GF(2^m) is presented. Based on several properties of the syndrome matrices, the new step-by-step decoding algorithm can directly determine whether every received symbol is an error locator. The detection of error location is based only on the determinant of a $v \times v$ syndrome matrix, where v is the number of errors. When an error location is found, its corresponding error value can also be determined by performing a determinant division operation between two syndrome matrices. The new decoding algorithm can significantly reduce computation complexity and improve the decoding speed compared with the conventional step-by-step decoding algorithm.

1 Introduction

Among the many error-correcting codes, Reed–Solomon (RS) codes are the most frequently employed in digital communication and storage systems. Many decoding techniques have been proposed for decoding RS codes, such as the Berlekamp-Massey algorithm [1–4], the Euclidean algorithm [1–5], and the step-by-step decoding algorithm [6, 7]. The step-by-step decoding algorithm was first presented by Massey in 1965. The difference between the step-by-step method and the standard algebraic method is that the step-by-step method decodes every potential error location and error value directly, instead of searching the error locators and evaluating the error values.

The conventional step-by-step decoding algorithm corrects the errors in terms of the differences between the original syndrome matrix and the temporarily changed syndrome matrices. This idea is based on the fact that the weight of error patterns can be distinguished from each other by using the syndrome matrices. Therefore, the conventional step-by-step algorithm adds in order all possible $2^m - 1$ nonzero elements of GF(2^m) to every symbol of the received word to determine whether the weight of the error pattern has been reduced. If the weight of the error pattern is reduced, both the error location and the corresponding error value are found. When the number of errors v in the received word is determined, the decoding procedure only needs to detect whether a determinant of the $v \times v$ changed syndrome matrix vanishes for every nonzero element of GF(2^m) added in every detected symbol. If the determinant vanishes, the detected symbol is an error and the added nonzero element is its error value. Compared with other decoding algorithms, the step-by-step algorithm offers the advantage of a simple decoding concept because the step-by-step algorithm only depends on a $v \times v$ syndrome matrix. However, $2^m - 1$ iterations must be performed for every received symbol in the conventional step-by-step decoding algorithm. In order to speed up the decoding process, a new step-by-step decoding algorithm is developed in this paper. In the new decoding algorithm, instead of trying every potential element, a new method for directly searching the error locators is presented. The new error locator searching method is based on several properties of the syndrome matrix to detect directly whether every received symbol is an error. The detection of error location is only based on whether a $v \times v$ syndrome matrix is singular or not, where v is the number of errors. When an error is found by the new searching method, the corresponding error value can easily be obtained by performing a determinant division operation of two syndrome matrices.

2 Properties of syndrome matrix

For a t-error-correcting RS code with symbols from the Galois field GF(2^m), the codeword can be expressed as

$$c(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1} \qquad (1)$$

Due to the presence of the channel noise, the received word $r(x)$ in the receiver may be different from the encoded codeword $c(x)$ in the transmitter. Let the error polynomial caused by the channel noise have the form

$$e(x) = e_0 + e_1x + e_2x^2 + \ldots + e_{n-1}x^{n-1} \qquad (2)$$

Then the received word can be expressed as

$$\begin{aligned} r(x) &= c(x) + e(x) \\ &= r_0 + r_1x + r_2x^2 + \ldots + r_{n-1}x^{n-1} \qquad (3) \end{aligned}$$

The weight of the error polynomial $e(x)$ would be the number of errors in the received polynomial $r(x)$. The syndrome values of a received word with v errors can be obtained from

$$\begin{aligned} S_i &= r(\alpha^i) \\ &= e(\alpha^i) \\ &= \sum_{j=1}^{v} Y_jX_j^i \qquad i = 1, 2, \ldots, 2t \end{aligned}$$

IEE Proceedings online no. 20000149

DOI: 10.1049/ip-com:20000149

Paper first received 1st February and in revised form 27th October 1999

T.-C. Chen and C.-H. Wei are with the Department of Electronics Engineering, National Chiao Tung University, Hsinchu, Taiwan 30050, Republic of China

S.-W. Wei is with the Department of Electrical Engineering, Chung Hua University, Hsinchu, Taiwan 30067, Republic of China

where X_j indicates the error location of the jth erroneous symbol and Y_j is the corresponding error value. Therefore, the decoding task is, given the syndrome values, to find the error locations and error values.

The conventional step-by-step decoding algorithm corrects the errors directly in terms of the difference between the original syndrome matrices and the temporarily changed syndrome matrices. The various weights of error patterns can be distinguished from the syndrome matrices. A $k \times k$ syndrome matrix, N_k, has the following relation with the syndrome values [2, 5–8]

$$N_k = \begin{bmatrix} S_1 & S_2 & \cdots & S_k \\ S_2 & S_3 & \cdots & S_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_k & S_{k+1} & \cdots & S_{2k-1} \end{bmatrix} \tag{4}$$

For t-error-correcting RS codes, the syndrome matrix N_k is singular if the number of errors in $r(x)$ is $k - 1$ or less; the syndrome matrix N_k is nonsingular if the number of errors is k [2, 5–8]. That is, the determinant of the syndrome matrix $\det(N_k)$ equals zero if the number of errors is $k - 1$ or less and $\det(N_k) \neq 0$ if the number of errors is k. The conventional step-by-step decoding algorithm adds in order all $2^m - 1$ nonzero elements of GF(2^m) to every symbol of the received word to determine whether the weight of the error pattern has been reduced. If the weight of the error pattern is reduced, both the error location and the corresponding error value are found.

For a received word $r(x)$, we add a nonzero element β of GF(2^m) to the first symbol r_0. Then the changed syndrome values, denoted as S'_i $1 \leq i \leq 2t$, will be

$$S'_i = S_i + \beta \tag{5}$$

and the changed syndrome matrices, denoted as N'_k, $1 \leq k \leq t$, can be expressed as

$$N'_k = \begin{bmatrix} S'_1 & S'_2 & \cdots & S'_k \\ S'_2 & S'_3 & \cdots & S'_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ S'_k & S'_{k+1} & \cdots & S'_{2k-1} \end{bmatrix}$$
$$= \begin{bmatrix} S_1+\beta & S_2+\beta & \cdots & S_k+\beta \\ S_2+\beta & S_3+\beta & \cdots & S_{k+1}+\beta \\ \vdots & \vdots & \ddots & \vdots \\ S_{k+\beta} & S_{k+1}+\beta & \cdots & S_{2k-1}+\beta \end{bmatrix} \tag{6}$$

Then the value of $\det(N'_k)$ can be obtained as

$$\det(N'_k) = \begin{vmatrix} S'_1 & S'_2 & \cdots & S'_k \\ S'_2 & S'_3 & \cdots & S'_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ S'_k & S'_{k+1} & \cdots & S'_{2k-1} \end{vmatrix}$$
$$= \begin{vmatrix} S_1 & S_2 & \cdots & S_k \\ S_2 & S_3 & \cdots & S_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ S_k & S_{k+1} & \cdots & S_{2k-1} \end{vmatrix} + \beta$$
$$\cdot \begin{vmatrix} S_1+S_3 & S_2+S_4 & \cdots & S_{k-1}+S_{k+1} \\ S_2+S_4 & S_3+S_5 & \cdots & S_k+S_{k+2} \\ \vdots & \vdots & \ddots & \vdots \\ S_{k-1}+S_{k+1} & S_k+S_{k+2} & \cdots & S_{2k-3}+S_{2k-1} \end{vmatrix} \tag{7}$$

Now, a new $k \times k$ syndrome matrix M_k is defined as

$$M_k = \begin{bmatrix} S_1+S_3 & S_2+S_4 & \cdots & S_k+S_{k+2} \\ S_2+S_4 & S_3+S_5 & \cdots & S_{k+1}+S_{k+3} \\ \vdots & \vdots & \ddots & \vdots \\ S_k+S_{k+2} & S_{k+1}+S_{k+3} & \cdots & S_{2k-1}+S_{2k+1} \end{bmatrix} \tag{8}$$

Then $\det(N'_k)$ can be expressed as

$$\det(N'_k) = \det(N_k) + \beta \cdot \det(M_{k-1}) \tag{9}$$

with initial value $\det(M_0) = 1$.

For the jth cyclic shifted polynomial of $r(x)$, denoted as

$$r^{(j)}(x) = r_{n-j} + r_{n-j+1}x + \ldots + r_{n-1}x^{j-1}$$
$$+ r_0 x^j + \ldots + r_{n-j-1}x^{n-1} \tag{10}$$

the corresponding syndrome values are denoted as S_i^j, $1 \leq i \leq 2t$. Similarly, the corresponding syndrome matrices can be expressed as

$$N_k^j = \begin{bmatrix} S_1^j & S_2^j & \cdots & S_k^j \\ S_2^j & S_3^j & \cdots & S_{k+1}^j \\ \vdots & \vdots & \ddots & \vdots \\ S_k^j & S_{k+1}^j & \cdots & S_{2k-1}^j \end{bmatrix} \tag{11}$$

and

$$M_k^j = \begin{bmatrix} S_1^j+S_3^j & S_2^j+S_4^j & \cdots & S_k^j+S_{k+2}^j \\ S_2^j+S_4^j & S_3^j+S_5^j & \cdots & S_{k+1}^j+S_{k+3}^j \\ \vdots & \vdots & \ddots & \vdots \\ S_k^j+S_{k+2}^j & S_{k+1}^j+S_{k+3}^j & \cdots & S_{2k-1}^j+S_{2k+1}^j \end{bmatrix} \tag{12}$$

Then, a nonzero element β is added to the first symbol r_{n-j} of $r^{(j)}(x)$ to obtain the new polynomial $r'^{(j)}(x)$ and the corresponding syndrome values S'^j_i, $1 \leq i < 2t$. Consequently, we can obtain the following equation

$$\det(N'^j_k) = \det(N_k^j) + \beta \cdot \det(M_k^j) \tag{13}$$

where

$$N'^j_k = \begin{bmatrix} S'^j_1 & S'^j_2 & \cdots & S'^j_k \\ S'^j_2 & S'^j_3 & \cdots & S'^j_{k+1} \\ \vdots & \vdots & \ddots & \vdots \\ S'^j_k & S'^j_{k+1} & \cdots & S'^j_{2k-1} \end{bmatrix} \tag{14}$$

Henceforth, in order to describe some theorems and the decoding algorithm for convenience, we let the notation $r^{(0)}(x) = r^{(n)}(x) = r(x)$ denote the initial received word $r(x)$ and $N_k{}^0$, $M_k{}^0$ denote the corresponding syndrome matrices.

Some properties of the new syndrome matrices are presented as follows.

Theorem 1: For a received word of (n, k, t) RS code, if the number of errors is v and $\det(M_{v-1}^j) = 0$, then the symbol r_{n-j} must be a correct symbol.

Proof: See the Appendix (Section 6.1).

Theorem 2: For an (n, k, t) RS code, if the number of errors in a received word $r(x)$ is $v < t$, then the symbol r_{n-j} is an erroneous symbol if and only if $\det(M_v^j) = 0$, $1 \leq j \leq n$. Otherwise, r_{n-j} must be a correct symbol.

Proof: See the Appendix (Section 6.2).

For a general t-error-correcting RS code, the number of errors v can be pre-determined by the syndrome matrices N_i, $i \le t$, as defined in eqn. 4. Based on theorem 1, r_{n-j} must be a correct symbol if the $(v-1) \times (v-1)$ syndrome matrix M_{v-1}^j is singular, i.e. $\det(M_{v-1}^j) = 0$. However, this theorem does not ensure that r_{n-j} is an erroneous symbol if $\det(M_{v-1}^j) \neq 0$. Based on theorem 2, r_{n-j} must be an error symbol if and only if the $v \times v$ syndrome matrix M_v^j is singular, i.e. $\det(M_v^j) = 0$. However, when $v = t$, S_{2t+1}, and hence M_t^j are not calculable. Therefore, when the error number of the received word $r(x)$ is equal to t, the $(t-1) \times (t-1)$ syndrome matrix M_{t-1}^j will be first detected. If $\det(M_{t-1}^j) = 0$, the symbol r_{n-j} must be a correct symbol. If $\det(M_{t-1}^j) \neq 0$, the symbol r_{n-j} may possibly be an erroneous symbol. Assuming that r_{n-j} is an erroneous symbol, we may find a nonzero element β in GF(2^m) to let the error number of $r'^{(j)}(x)$ become $t-1$. That is, $\det(N'^j_t) = \det(N'^j_{t+1}) = 0$. Based on the equation

$$\det(N_t'^j) = \det(N_t^j) + \beta \cdot \det(M_{t-1}^j) = 0$$

only the nonzero element $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ would let $\det(N'^j_t) = 0$. If the nonzero element $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ can also let $\det(N'^j_{t+1}) = 0$, then the symbol r_{n-j} is an erroneous symbol and the value $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ is the corresponding error value. Although S'^j_{2t+1}, and hence $\det(N'^j_{t+1})$, are not calculable for a t-error-correcting RS code. However, $\det(N'^j_t)$ equals zero and is the cofactor of S'^j_{2t+1} in the syndrome matrix N'^j_{t+1}. The value of $\det(N'^j_{t+1})$ is independent of S'^j_{2t+1} and can thus be obtained. Therefore, if the number of errors in $r(x)$ is t, we first calculate the value $\det(M_{t-1}^j)$; if $\det(M_{t-1}^j) = 0$, then the symbol r_{n-j} is a correct symbol; if $\det(M_{t-1}^j) \neq 0$, then let $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ and calculate the value $\det(N'^j_{t+1})$. If $\det(N'^j_{t+1}) = 0$, r_{n-j} is an error symbol and $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ is the corresponding error value. Consequently, we have the following corollary.

Corollary 1: For a received word of (n, k, t) RS code and number of errors $v = t$, the symbol r_{n-j} must be an erroneous symbol if and only if a unique nonzero value $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ exists such that $\det(N'^j_{t+1}) = 0$.

Based on theorem 2 and corollary 1, the error locations can be found symbol-by-symbol. Then, the corresponding error values can easily be obtained from the following theorem.

Theorem 3: For a received word of (n, k, t) RS code, if the number of errors is v and the symbol r_{n-j} is an erroneous symbol, then $\det(M_{v-1}^j) \neq 0$ and the corresponding error value is $\det(N_v^j)/\det(M_{v-1}^j)$.

Proof: See the Appendix (Section 6.3).

3 New step-by-step decoding algorithm

Based on the syndrome matrices and the new method for searching the error locations and error values, a new step-by-step decoding algorithm is presented. First, the syndrome values S_i^0, $i = 1, 2, ..., 2t$, and syndrome matrices N_k^0, $k = 1, 2, ..., t$, of the received word $r(x)$ are calculated to determine the number of errors (i.e., the value of v). For a general t-error-correcting RS code, the number of errors can be determined by just consecutively testing $\det(N_t^0)$, $\det(N_{t-1}^0)$, ..., until a nonzero determinant, say $\det(N_v^0)$, is found [6]. When the error number v is known, the new algorithm tests every symbol of $r(x)$ step-by-step to detect whether or not it is an error. If an error locator is found, its error value can easily be obtained by calculating $\det(N_v^j)/\det(M_{v-1}^j)$. Based on these properties of syndrome matrices, two types of the new decoding algorithm, the parallel version and sequential version, are presented as follows.

3.1 Parallel decoding algorithm

Step 1: Calculate the initial syndrome values S_i^0 ($i = 1, 2, ..., 2t$) and the determinants of the initial syndrome matrices $\det(N_k^0)$ ($k = 1, 2, ..., t$) from the received word $r^{(0)}(x) = r(x) = r_0 + r_1x + r_2x^2 + ... + r_{n-1}x^{n-1}$. Then determine the number of errors v.

Step 2: If $v = 0$, go to step 7.

Step 3: Calculate the syndrome values $S_i^j = S_i^0 \cdot \alpha^{ij}$, $1 \le i \le 2v$, and the determinants $\det(N_k^j) = \alpha^{jk^2} \cdot \det(N_k^0)$ for all j [see the Appendix (Sections 6.4 and 6.5)].

Step 4: If $v = t$, go to step 6.

Step 5: Calculate the value $\det(M_v^j)$, $1 \le j \le n$. For all j, if $\det(M_v^j) = 0$, let $r_{n-j} = r_{n-j} + \det(N_v^j)/\det(M_{v-1}^j)$. Go to step 7.

Step 6: Calculate $\det(M_{t-1}^j)$, $1 \le j \le n$. For all j, if $\det(M_{t-1}^j) \neq 0$, let $\beta_{n-j} = \det(N_t^j)/\det(M_{t-1}^j)$ and calculate the determinant $\det(N_{t+1}^j)$. For all j, if $\det(M_{t-1}^j) \neq 0$ and $\det(N_{t+1}^j) = 0$, let $r_{n-j} = r_{n-j} + \det(N_t^j)/\det(M_{t-1}^j)$.

Step 7: The decoding algorithm has been completed.

3.2 Sequential decoding algorithm

Step 1: Calculate the initial syndrome values S_i^0 ($i = 1, 2, ..., 2t$) and determine the number of errors v from $\det(N_k^0)$ ($k = 1, 2, ..., t$).

Step 2: If $v = 0$, go to step 13.

Step 3: Let $j = 1$.

Step 4: Calculate the syndrome values $S_i^j = S_i^{j-1} \cdot \alpha^i$, $i = 1, 2, ..., 2v - 1$, and the determinants $\det(N_k^j) = \alpha^{k^2} \cdot \det(N_k^{j-1})$, $k = 1, 2, ..., v$. [see the Appendix (Sections 6.4 and 6.5)].

Step 5: If $v < t$, go to step 11.

Step 6: Calculate $\det(M_{t-1}^j)$ from the syndrome values S_i^j.

Step 7: If $\det(M_{t-1}^j) = 0$, go to step 13.

Step 8: Let $\beta = \det(N_t^j)/\det(M_{t-1}^j)$ and $r'_{n-j} = r_{n-j} + \beta$.

Step 9: Let $S'^j_i = S_i^j + \beta$, $i = 1, 2, ..., 2t$, and calculate $\det(N'^j_{t+1})$.

Step 10: If $\det(N'^j_{t+1}) \neq 0$, go to step 13. Otherwise, calculate $\det(M_k^j)$, $k = 1, 2, ..., t-2$, and let $v = v - 1$, $r_{n-j} = r'_{n-j}$, $S_i^j = S'^j_i$, $\det(N_k^j) = \det(N_k^j) + \beta \cdot \det(M_{k-1}^j)$, $k = 1, 2, ..., v$. Go to step 13.

Step 11: Calculate the value $\det(M_v^j)$.

Step 12: If $\det(M_v^j) \neq 0$, go to step 13. Otherwise, calculate the values $\det(M_k^j)$, $k = 1, 2, ..., v - 1$, and let $\beta = \det(N_v^j)/\det(M_{v-1}^j)$, $r_{n-j} = r_{n-j} + \beta$, $S_i^j = S_i^j + \beta$, $v = v - 1$, $\det(N_k^j) = \det(N_k^j) + \beta \cdot \det(M_{k-1}^j)$, $k = 1, 2, ..., v$.

Step 13: If $j = n$ or $v = 0$, then this decoding algorithm is completed. Otherwise, let $j = j + 1$ and go to step 4.

The new decoding algorithm can also be applied in decoding shortened RS codes. Consider a $(n - l, k - l, t)$ shortened RS code, the encoded codeword $c(x)$ and the received word $r(x)$ can be expressed, respectively, as

$$c(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-l-1}$$

and

$$r(x) = r_0 + r_1x + r_2x^2 + \ldots + r_{n-1}x^{n-l-1}$$

For the parallel decoding, only replace '$1 \le j \le n$' by '$l + 1 \le j \le n$' for all steps. For the sequential decoding, just modify step 3 as follows:

Step 3: Calculate $S_i^j = S_i^0 \cdot \alpha^{il}$, $1 \le i \le 2v - 1$, and $\det(N_k^j) = \alpha^{lk^2} \cdot \det(N_k^0)$. Let $j = l + 1$.

Because the new decoding algorithm is performed symbol-by-symbol, the computation complexity can be reduced for the shortened codes.

4 Conclusions

The conventional step-by-step decoding algorithm corrects the errors in terms of the differences between the original syndrome matrices and the temporarily changed syndrome matrices. Compared with the other decoding algorithms, the step-by-step algorithm offers the advantage of a simple decoding process which depends on calculating $\det(N'^j_v)$ (and $\det(N'^j_{t+1})$ if $v = t$). However, the conventional step-by-step algorithm must perform $2^m - 1$ iterations to detect the determinant $\det(N'^j_v)$ (and $\det(N'^j_{t+1})$ if $v = t$) for every received symbol. In order to speed up the decoding process, a new step-by-step decoding algorithm has been presented. A new syndrome matrix M_k was developed. Based on some properties of the syndrome matrices, a new method for searching the error locations and the corresponding error values has also been presented. The new step-by-step decoding algorithm only detects the determinant of the $v \times v$ matrix $\det(M^j_v)$ once for every received symbol (it detects $\det(M^j_{t-1})$ and $\det(N^j_{t+1})$ if $v = t$). Compared with the conventional step-by-step algorithm, the new algorithm reduces the computational complexity by a factor of $2^m - 1$. Based on the new step-by-step decoding method, a parallel decoding algorithm and a sequential decoding algorithm have been proposed. The parallel decoding algorithm detects all received symbols to obtain the corresponding error pattern in parallel. Thus, a high-speed parallel decoder can be constructed to perform the decoding process in the interval of one iteration, which is particularly suitable for shortened RS codes. The sequential decoding algorithm tests one symbol at a time. The decoder has lower circuit-complexity and can complete the decoding process with n iterations.

5 References

1 LIN, S., and COSTELLO, D.: 'Error control coding: fundamentals and applications' (Prentice Hall, Englewood Cliffs, NJ, 1983)

2 BLAHUT, R.E.: 'Theory and practice of error control codes' (Addison-Wesley, New York, 1983)

3 CLARK, G.C., and CAIN, J.B.: 'Error-correcting coding for digital communications' (Plenum, New York, 1981)

4 MICHELSON, A.M., and LEVESQUE, A.H.: 'Error-control techniques for digital communication' (Wiley, New York, 1985)

5 PETERSON, W.W., and WELDON, E.J.: 'Error-correcting codes' (MIT Press, Cambridge, 1972, 2nd edn.)

6 MASSEY, J.L.: 'Step-by-step decoding of the Bose-Chaudhuri-Hocquenghem codes', *IEEE Trans. Inf. Theory*, 1965, **IT-11**, (4), pp. 580–585

7 WEI, S.W., and WEI, C.H.: 'High-speed decoder of Reed-Solomon codes', *IEEE Trans. Commun.*, 1993, 41, (11), pp. 1588–1593

8 JU, S., and BI, G.: 'Fast decoding algorithm for RS codes', *Electron. Lett.*, 1997, 33, (17), pp. 1452–1453

6 Appendix A

6.1 Proof of theorem 1

The number of errors v can be pre-determined by the syndrome matrices N_i, $i \leq t$ as defined in eqn. 4. Based on the property of cyclic codes, the number of errors in $r^{(j)}(x)$ is also v, and then $\det(N^j_v) \neq 0$. By adding a nonzero element β to r_{n-j}, we obtain the new polynomial $r'^{(j)}(x)$. From eqn. 13, we have

$$\det(N'^j_v) = \det(N^j_v) + \beta \cdot \det(M^j_{v-1})$$

If the symbol r_{n-j} is an erroneous symbol, the corresponding error value must be found, and also $\det(N'^j_v) = 0$. However, for all nonzero elements in $GF(2^m)$, it is impossible to have the relation $\det(N'^j_v) = 0$ because $\det(N^j_v) \neq 0$ and $\det(M^j_{v-1}) = 0$. Therefore, the symbol r_{n-j} must be a correct symbol if $\det(M^j_{v-1}) = 0$.

6.2 Proof of theorem 2

First, we add an arbitrary nonzero element β from $GF(2^m)$ to the symbol r_{n-j} to obtain a new polynomial $r'^{(j)}(x)$. If r_{n-j} is a correct symbol, the number of errors in $r'^{(j)}(x)$ should be $v + 1$. If r_{n-j} is an erroneous symbol, the number of errors in $r'^{(j)}(x)$ would be $v - 1$ (β is the error value) or v (β is not the correct error value). Based on eqn. 13:

$$\det(N'^j_{v+1}) = \det(N^j_{v+1}) + \beta \cdot \det(M^j_v)$$

Because $\det(N^j_{v+1}) = 0$ and $\beta \neq 0$, $\det(N'^j_{v+1}) \neq 0$ if and only if $\det(M^j_v) \neq 0$. That is, the symbol r_{n-j} is a correct symbol originally and then the nonzero element β is added to let the error number of $r'^{(j)}(x)$ become $v + 1$ if and only if $\det(M^j_v) \neq 0$. On the other hand, $\det(N'^j_{v+1}) = 0$ if and only if $\det(M^j_v) = 0$. This means that the error number of $r'^{(j)}(x)$ is less than $v + 1$. That is, the symbol r_{n-j} is an erroneous symbol originally and then the nonzero element β is added to let the error number of $r'^{(j)}(x)$ be v or $v - 1$, and thus $\det(N'^j_{v+1}) = 0$ if and only if $\det(M^j_v) = 0$.

6.3 Proof of theorem 3

Suppose that the symbol r_{n-j} is an erroneous symbol and let the nonzero element β in $GF(2^m)$ be its corresponding error value. Then adding the error value β to r_{n-j} will reduce the error number of $r'^{(j)}(x)$ to $v - 1$ and thus

$$\det(N'^j_v) = \det(N^j_v) + \beta \cdot \det(M^j_{v-1}) = 0$$

Because $\det(N^j_v) \neq 0$ and $\beta \neq 0$, $\det(M^j_{v-1}) \neq 0$ must be true and $\beta = \det(N^j_v)/\det(M^j_{v-1})$ is the only possible solution. Therefore, if the symbol r_{n-j} is an error symbol, then $\det(M^j_{v-1})$ cannot be equal to zero and the corresponding error value must be $\det(N^j_v)/\det(M^j_{v-1})$.

6.4 Calculation of syndrome values

The syndrome values S^j_i, $1 \leq i \leq 2t$, can be obtained from S^0_i or S^{j-1}_i by performing the following operations:

$$S^j_i = \alpha^{ij} \cdot S^0_i \quad \text{and} \quad S^j_i = \alpha^i \cdot S^{j-1}_i, \quad 1 \leq i \leq 2t$$

Proof:

$$\begin{aligned} S^j_i &= r^{(j)}(x)\big|_{x=\alpha^i} \\ &= r_{n-j} + r_{n-j+1}x + \ldots + r_{n-1}x^{j-1} \\ &\quad + r_0x^j + \ldots + r_{n-j-1}x^{n-1}\big|_{x=\alpha^i} \\ &= r_{n-j} + r_{n-j+1}\alpha^i + \ldots + r_{n-1}\alpha^{(j-1)\cdot i} \\ &\quad + r_0\alpha^{j\cdot i} + \ldots + r_{n-j-1}\alpha^{(n-1)\cdot i} \end{aligned} \tag{15}$$

For $GF(2^m)$, $\alpha^{2^m-1} = \alpha^n = 1$ and $(\alpha^n)^i = \alpha^{n\cdot i} = 1$.

Then

$$\begin{aligned} S^j_i &= \alpha^{n\cdot i}\left(r_{n-j} + r_{n-j+1}\alpha^i + \ldots + r_{n-1}\alpha^{(j-1)\cdot i}\right) \\ &\quad + r_0\alpha^{j\cdot i} + \ldots + r_{n-j-1}\alpha^{(n-1)\cdot i} \\ &= r_0\alpha^{j\cdot i} + \ldots + r_{n-j-1}\alpha^{(n-1)\cdot i} + r_{n-j}\alpha^{n\cdot i} \\ &\quad + \ldots + r_{n-1}\alpha^{(n+j-1)\cdot i} \\ &= \alpha^{j\cdot i} \cdot \left(r_0 + r_1\alpha + \ldots + r_{n-1}\alpha^{(n-1)\cdot i}\right) \\ &= \alpha^{ij} \cdot S^0_i \end{aligned} \tag{16}$$

Similarly

$$S^{j-1}_i = \alpha^{i\cdot(j-1)} \cdot S^0_i \tag{17}$$

Therefore

$$S^j_i = \alpha^{ij} \cdot S^0_i = \alpha^i \cdot \left(\alpha^{i\cdot(j-1)} \cdot S^0_i\right) = \alpha^i \cdot S^{j-1}_i \tag{18}$$

6.5 Calculation of determinants

It is complex to directly calculate the determinants of the syndrome matrices

$$\det(N_k^j) = \begin{vmatrix} S_1^j & S_2^j & S_3^j & \cdots & S_k^j \\ S_2^j & S_3^j & S_4^j & \cdots & S_{k+1}^j \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_k^j & S_{k+1}^j & S_{k+2}^j & \cdots & S_{2k-1}^j \end{vmatrix}$$

$$1 \le i \le t \qquad (19)$$

The determinants $\det(N_k^j)$, $1 \le i \le t$, can be easily obtained from $\det(N_k^0)$ or $\det(N_k^{j-1})$ as follows:

$$\det(N_k^j) = \alpha^{j \cdot k^2} \cdot \det(N_k^0)$$

$$\text{and } \det(N_k^j) = \alpha^{k^2} \cdot \det(N_k^{j-1})$$

Proof:

$$\det(N_k^j) =$$

$$\begin{vmatrix} \alpha S_1^{j-1} & \alpha^2 S_2^{j-1} & \alpha^3 S_3^{j-1} & \cdots & \alpha^k S_k^{j-1} \\ \alpha^2 S_2^{j-1} & \alpha^3 S_3^{j-1} & \alpha^4 S_4^{j-1} & \cdots & \alpha^{k+1} S_{k+1}^{j-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha^k S_k^{j-1} & \alpha^{k+1} S_{k+1}^{j-1} & \alpha^{k+2} S_{k+2}^{j-1} & \cdots & \alpha^{2k-1} S_{2k-1}^{j-1} \end{vmatrix}$$

$$= \alpha \cdot \alpha^2 \cdots \alpha^k$$

$$\cdot \begin{vmatrix} S_1^{j-1} & \alpha S_2^{j-1} & \alpha^2 S_3^{j-1} & \cdots & \alpha^{k-1} S_k^{j-1} \\ S_2^{j-1} & \alpha S_3^{j-1} & \alpha^2 S_4^{j-1} & \cdots & \alpha^{k-1} S_{k+1}^{j-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_k^{j-1} & \alpha S_{k+1}^{j-1} & \alpha^2 S_{k+2}^{j-1} & \cdots & \alpha^{k-1} S_{2k-1}^{j-1} \end{vmatrix}$$

(The factors α, α^2, ..., α^k are extracted in order for every row.)

$$= (\alpha \cdot \alpha^2 \cdots \alpha^k) \cdot (\alpha \cdot \alpha^2 \cdots \alpha^{k-1})$$

$$\cdot \begin{vmatrix} S_1^{j-1} & S_2^{j-1} & S_3^{j-1} & \cdots & S_k^{j-1} \\ S_2^{j-1} & S_3^{j-1} & S_4^{j-1} & \cdots & S_{k+1}^{j-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_k^{j-1} & S_{k+1}^{j-1} & S_{k+2}^{j-1} & \cdots & S_{2k-1}^{j-1} \end{vmatrix}$$

(The factors 1, α, α^2, ..., α^{k-1} are extracted in order for every column.)

$$= \alpha^{\frac{k(k+1)}{2} + \frac{(k-1)k}{2}}$$

$$\cdot \begin{vmatrix} S_1^{j-1} & S_2^{j-1} & S_3^{j-1} & \cdots & S_k^{j-1} \\ S_2^{j-1} & S_3^{j-1} & S_4^{j-1} & \cdots & S_{k+1}^{j-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ S_k^{j-1} & S_{k+1}^{j-1} & S_{k+2}^{j-1} & \cdots & S_{2k-1}^{j-1} \end{vmatrix}$$

$$= \alpha^{k^2} \cdot \det(N_k^{j-1}) \qquad (20)$$

Similarly,

$$\begin{aligned} \det(N_k^j) &= \alpha^{k^2} \cdot \det(N_k^{j-1}) \\ &= \alpha^{k^2} \cdot \left(\alpha^{k^2} \cdot \det(N_k^{j-2})\right) \\ &= \alpha^{2 \cdot k^2} \cdot \det(N_k^{j-2}) \\ &\vdots \\ &= \alpha^{j \cdot k^2} \cdot \det(N_k^0) \end{aligned} \qquad (21)$$