Performance Evaluation of Reed-Solomon Coded Single Carrier Signal

Prof. Dr W. A. Mahmmoud*, Samah Abdul-Kareem & Prof. Dr. N. K. Wafi***

Received on: 24/5/2004
Accepted on: 28/4/2005

Abstract

In this paper, Reed-Solomon coding and modulation are combined and analyzed in single carrier system over AWGN and Rician fading channel. The Simulation results are presented under different conditions using M-DPSK and M-QAM multilevel modulation. It is found that RS coded QAM signal performs better than the coded D-PSK signal with the same modulation size. Also, lower BER over fading channel is recoded by using more error code correction capability and/or shorter code word.

الخلاصة

في هذا البحث، تم ضم شفرة ريد- سولومون مع التضمين في نظام أحادي الحامل و تحليلها في القناة المضيفة للضوضاء وقناة الخبو راسين. نتائج التحليل مثلت تحت ظروف مختلفة وباستخدام مضمنات متعددة المستويات M-DPSK و M-QAM. لقد وجدت بان اشارة التضمين QAM المشفرة تبدي أداء أفضل من الأشارة ذو تضمين D-PSK مع نفس حجم التضمين. كما أن معدلات خطأ أقل قد تم تسجيله على قناة الخبو باس خدام قابلية تصحيح شفرة أكبر او\ و شفرات أقصر.

I. Introduction

Due to the fading characteristic of the wireless channel, the errors usually exhibit bursty pattern. Although, most existing channel codes do not work well with burst errors, an efficient approach is to use Reed-Solomon (RS) code. It is Originally conceived in 1960, by mathematicians Irving Reed and Gustave Solomon [Riley & Richardson 1997].

Reed-Solomon (RS) code is a cyclic symbol error-correcting code that operates at the block level rather than the bit level. For block codes, the incoming data stream is first packaged into small blocks. These blocks are then treated as a new set of k symbols to be packaged into a super-coded block of n symbols, by appending the calculated redundancy. Such symbols can either be comprised of one bit (binary code) or, of several bits (symbol codes). Therefore, the information transfer rate is reduced by a factor called code rate $R= k/n$, and the bandwidth of the signal produced by the modulator is expanded by the ratio $1/R= n/k$, relative to a system using the same modulator without coding [Riley & Richardson 1997].

RS codes are often used in mobile radio systems where burst errors are common, either as an alternative to, or in addition to interleaving, such as DVB/DAB broadcasting, Internet and mobile Internet communications [Xu & Zhang 2002].

The RS encoding and decoding require a considerable amount of computation and arithmetical operations over a finite number system with certain properties, i.e. algebraic systems, which in this case is called fields. RS's initial definition focused on the evaluation of polynomials over the elements in a finite field (Galois

*University of Baghdad
**University of Salahaddin

field *GF*) [Blahut 1985]. Others have preferred to examine RS codes in light of the Galois field Fourier transform [Riley & Richardson 1997]. The simulation here is based on the first definition.

In this paper, sections II & III provide a representation of RS encoding and decoding process, respectively. Shortened RS code is explained in section IV, and convolutional interleaver is described in section V. Section VI & VII present the evaluated coded single carrier system and Rician channel model, respectively. The simulation results are available in section VIII. Finally, the conclusions are provided in section IX.

II. RS Encoding Procedure

The implemented procedure to construct a t-error correction RS code of length $n=q-1$ over $GF(q)$ for which the symbols are belong, can be established in a flowchart as illustrated in figure (1).

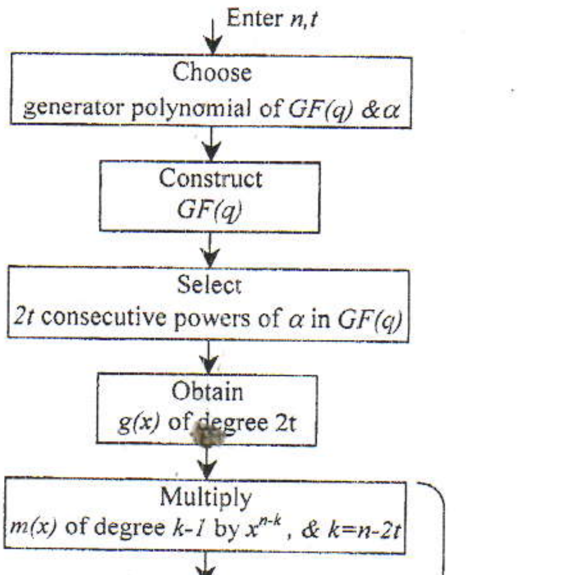

Figure (1): Flowchart of RS code construction procedure.

For a t symbol-error correcting capability RS code, the generator polynomial over $GF(q)$ can be expressed as

$$g(x)=(x-\alpha^{j0})(x-\alpha^{j0+1})..(x-\alpha^{j0+2t-1}) \qquad (1)$$

Often one chooses $j_o=1$, which is usually-but-not always. α is the primitive element of $GF(q)$ and $g(x)$ is always a polynomial of degree of $2t$ [Blahut 1985]. Hence, an RS code satisfies $n-k=2t$, where $n=q-1$ is the length of a code word in symbols and k is the number of information symbol. Whereas the block length of the code is tied to the field size, the dimension k may be selected as any integer up to $n-1$. As obvious, an (n,k) RS code always has minimum distance equal to $n-k+1=2t+1$. This is often a strong justification for using RS code, It provides intrinsic robustness to burst error phenomena.

A given sequence of k information symbols in $GF(q)$, $M=[m_o, m_1, \ldots, m_{k-1}]$, can be represented by a polynomial as $m(x)=m_0+m_1x+\ldots+m_{k-1}x^{k-1}$. The idea of the systematic encoding [Blahut 1985] that illustrated in figure (1), is to insert the information into the high-order coefficients of the code word, and the code word becomes in the form

$$c(x)=x^{n-k}m(x)+p(x) \qquad (2)$$

as depicted, the encoding procedure needs to find the parity check polynomial $p(x)$ by the division algorithm, using $m(x)$ and $g(x)$. To be an RS code $c(x)$ must be also a multiple of $g(x)$, and $p(x)$ is chosen so that:

$$R_{g(x)}[c(x)]=0 \qquad (3)$$

here $R_{g(x)}[c(x)]$ denotes the remainder of dividing $c(x)$ by $g(x)$. Then

$$R_{g(x)}[x^{n-k}m(x)]+R_{g(x)}[p(x)]=0 \qquad (4)$$

but the degree of $p(x)$ is $n-k$ and less than the degree of $g(x)$

$$p(x)=-R_{g(x)}[x^{n-k}m(x)] \qquad (5)$$

III. RS Decoding Procedure

If binary channel errors are confined to m bits and properly phased relative to symbol boundaries, the RS decoder sees these bursts as symbol errors in $GF(q)$, so a burst is no worse than an isolated bit error and the receiver still to be able to reinstate the correct information. The received symbol field is the same as the transmitted field, $GF(q)$.

RS codes are specified as codes that have $2t$ consecutive roots in $GF(q)$ with length $q-1$, then it can locate and correct up to t errors. RS decoding procedure is depicted in figure (2) [Blahut 1985]. Assume that the code word was transmitted and corrupted during transmission with an error signal e, and the received signal r becomes in the form

$$r(x)=c(x)+e(x) \qquad (6)$$

and suppose there are v errors in positions $i_1, i_2, \dots, i_v$ whose error magnitudes are $e_{il}, l=1,2,\dots,v$ respectively, and given by the error polynomial:

$$e(x)=e_{i1}x^{i1}+e_{i2}x^{i2}+\dots\dots+e_{iv}x^{iv} \qquad (7)$$

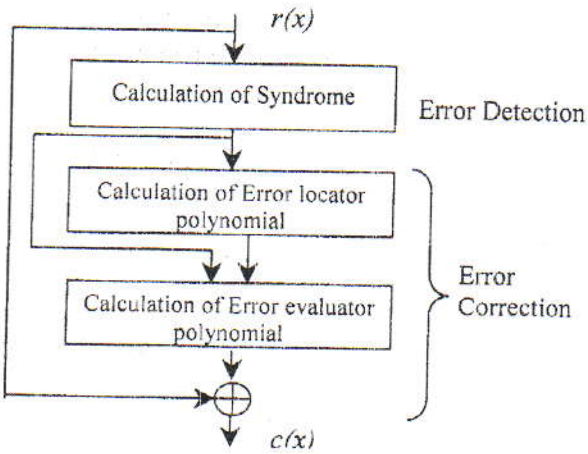

Figure (2): Flowchart of RS decoding procedure.

The decoder proceeds to evaluate the received polynomial $r(x)$ at the $2t$ roots $(\alpha, \alpha^2, \dots, \alpha^{2t})$ of the generator polynomial and compute the syndromes S_i, $i=1,2,\dots,2t$.

$$S_i = r(\alpha^i) = c(\alpha^i) + e(\alpha^i)$$
$$S_i=e(\alpha^i) \qquad (8)$$

The syndrome is used to calculate the error locator polynomial $\lambda(x)$ as given by

$$\begin{bmatrix} \lambda_v \\ \lambda_{v-1} \\ \vdots \\ \lambda_1 \end{bmatrix} = \begin{bmatrix} -S_{v+1} \\ -S_{v+2} \\ \vdots \\ -S_{2v} \end{bmatrix} \begin{pmatrix} S_1 & S_2 & \dots & S_{v-1} & S_v \\ S_2 & S_3 & \dots & S_v & S_{v+1} \\ \vdots & \vdots & & \vdots & \vdots \\ S_v & S_{v+1} & \dots & S_{2v-1} & S_{2v} \end{pmatrix}^{-1} \qquad (9)$$

where

$$\lambda(x)=\lambda_v x^v+\lambda_{v-1}x^{v-1}+\dots+\lambda_1 x+1 \qquad (10)$$
$$=(1-\alpha^{i1}x)(1-\alpha^{i2}x)\dots(1-\alpha^{iv}x) \qquad (11)$$

Then, the syndrome and the roots of error locator polynomial are used to obtain the error magnitude. In matrix form

$$\begin{bmatrix} e_{i1} & e_{i2} & \dots & e_{iv} \end{bmatrix} = \begin{bmatrix} S_1 & S_2 & \dots & S_{2t} \end{bmatrix} \begin{pmatrix} \alpha^{i1} & \alpha^{2i1} & \dots & \alpha^{2t\,i1} \\ \alpha^{i2} & \alpha^{2i2} & \dots & \alpha^{2t\,i2} \\ \vdots & \vdots & & \vdots \\ \alpha^{iv} & \alpha^{2iv} & \dots & \alpha^{2t\,i2} \end{pmatrix}^{-1}$$

(12)

The algorithm and its prove might be better understood by working through the details in appendix A. Last, GF addition of the error magnitude to the received word at the appropriate coordinates depending on the obtained error locator polynomial, output the corrected word.

IV. Shortened RS Codes

Given an (n,k) RS code as a mother code, a variety of RS codes $(n`,k`)$ can be derived from the mother code to fit different applications and universal encoder and decoder on chips can be used for different applications. The systematic RS code can be shortened, that is changed from an (n,k) code to an $(n-b,k-b)$ code by dropping b information symbols from each code word, without decreasing minimum distance or changing $n-k$. However, the shortened code may have a large minimum distance than the original code, and can also correct burst errors of length t (or longer) [Xu & Zhang 2002].

The same encoding and decoding procedure can be applied on the shortened codes with minor modification. In such codes, the unused b symbols in a shortened code are always set to zero, they need not be transmitted, but the receiver begin decoding by first stuffing zero symbols into the erased positions and continue just as if the code were not shortened.

V.Convolutional Interleaving Scheme

Interleaving and complementary deinterleaving in the receiver is a process for decorrelating burst errors, extending the power of coding schemes to a larger number of errors. The interleaver supplies no additional error correction code, it merely initiates a rearangement of the symbols generated by the encoder. A more efficient scheme is performed, according to [Reimers 2001], by the **convolutional interleaver** as shown in figure (3).

Figure (3): Block diagram of convolutional (de) interleaver.

It consists of I-1 shift registers with the length A, $2A$,..., and $A(I$-$1)$ and corresponding multiplexers and demultiplexers (represented as switches). I is the interleaver depth and the base delay $A=n/I$, where n , as before, the code word length. The next symbol is read into the shift register currently connected to the input, and another symbol is picked up from the output of that shift register. The I positions of code symbols are delayed by progressively larger amounts at the encoder output prior to transmission. This ensures that, between adjacent symbols at the input, $A.I$ further symbols are transmitted.

The total memory is only $I.A$ symbols, and the end-to-end delay is $I.A$ channel time units. The delay schedule is reversed at the demodulator output to bring the symbols into proper time alignment for decoding.

VI. Evaluated RS Coded Single Carrier System

Suppose we are dealing with a 256-level RS code of a natural block length 255 in conjunction with a modulation/demodulation scheme. Here the field size is 256, and the information and code symbols can be regarded as 8-bit symbols. Let that we seek a d_{min}=17, producing t=8 or fewer symbol-error-correcting capability. This implies that n-k=16, or the number of information symbols is 239.The generator polynomial for (255,239) RS code is a 16 degree polynomial over *GF(256)* with coefficients given in an ascending order as $\alpha^{136}\ \alpha^{240}\ \alpha^{208}\ \alpha^{195}\ \alpha^{181}\ \alpha^{158}\ \alpha^{201}\ \alpha^{100}\ \alpha^{11}\ \alpha^{83}\ \alpha^{167}\ \alpha^{107}\ \alpha^{113}\ \alpha^{110}\ \alpha^{106}\ \alpha^{121}\ 1$. The field generator polynomial for this code over *GF(2)* is $x^8+x^4+x^3+x^2+1$.

In such applications, there is one obvious method to avoid the traditional bandwidth expansion by a factor 255/239 associated with coding, which is to increase the number of symbol states in the modulation scheme. For this reason, spectrally efficient multilevel modulation schemes such as M-PSK and M-QAM were developed. However, increasing the number of symbol states may incur an implementation penalty as well as a large energy efficiency penalty, requiring higher phase and amplitude accuracy in both transmitter and receiver systems.

The performance of RS code is tested by combining channel and modulation coding in single carrier system, through the simulation of such a system as depicted in figure (4). The RS coded data are interleaved to provide additional error correction. This process spreads the data from several RS blocks over a much longer period of time so that long burst of noise is required to overcome the capability of the RS code.

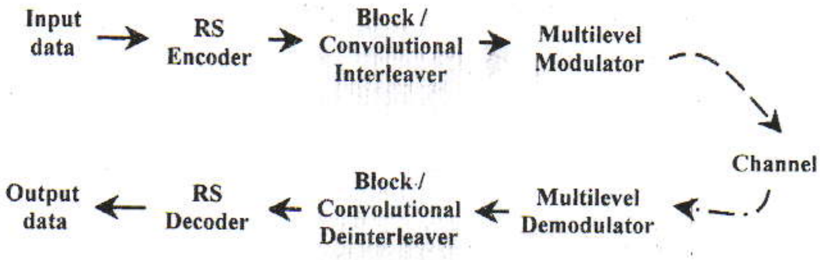

Figure (4): Block diagram of coded single carrier system model.

VII. Rician Channel Model

A Rician fading channel is characterized by a direct line of sight (LOS) and a multi-path components with a relative delay that create some inter-symbol interference ISI on the received signal. In such a channel, the multipath component is relatively small compared to the LOS component, and the output signal *y(n)* of the channel is described as a function of the input signal *x(n)*

$$y(n) = \frac{a_o\, x(n) + \sum_{i=1}^{K} a_i\ x(n-\tau_i)\, e^{j\theta_i}}{\sqrt{\sum_{i=0}^{K} a_i^{\,2}}} \tag{13}$$

where a_o is the attenuation in direct path and a_i, θ_i & τ_i are the attenuation, phase rotation and relative delay time in reflection path *i*. *K* denotes the number of reflection [Reimers 2001]. Also, the Maximum Excess Delay and Mean Excess Delay can be used to describe the behavior of the fading channel. Maximum Excess Delay corresponds to the delay associated with last arriving signal components compared to the initial delay or $(\tau_{K-1}-\tau_o)$ and the Mean Excess Delay is equivalent to the normalized first moment of the power delay profile in the form

$$\tau_{MED} = \frac{\sum_{n=-\infty}^{\infty} n\left|h(n)\right|^2}{\sum_{n=-\infty}^{\infty}\left|h(n)\right|^2} = \frac{\sum_{i=1}^{K} a_i^2 \tau_i}{\sum_{i=0}^{K} a_i^2} \quad (14)$$

VIII. Simulation Results

Differential M-DPSK and coherent M-QAM modulation/demodulation technique are adopted in this work. Figure (5) simulates the transmission of encoded and modulated single carrier signal in the presence of additive white Gaussian noise, where the encoded data are 15 symbols depth interleaved.

BER remains at high value until SNR exceeds a certain point dependent on the constellation size. As sequence of points from a bandwidth-efficient constellation, we can have a few positions where code words differ by symbols having large inter-signal distance, or we can have a relatively larger number of positions where the symbol distance is small. Ultimately, minimum distance between constellation points results in higher required SNR to achieve error-free reception, for example, a change from 64-DPSK to 128-DPSK results in a necessary increase in SNR by a maximum of 6dB. Moreover, it is clear that the coherent modulation performs better than differential modulated signal with the same constellation size of about 12 dB.

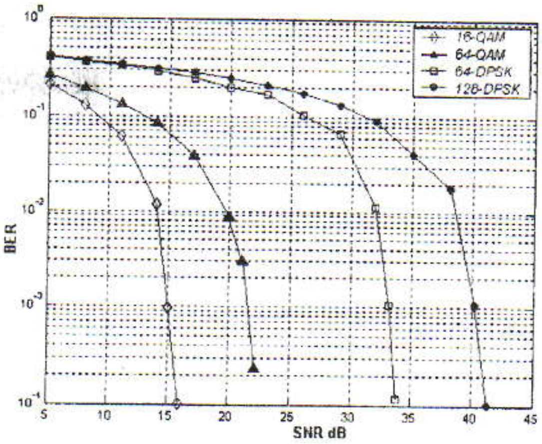

Figure (5): BER performance of single carrier system in AWGN channel with RS (255,239) code.

For inclusion of ISI effect on system performance under consideration due to multi-path propagation, figure (6) illustrates the BER as a function of SNR over Rician fading channel with two path and τ_{MED} of approximately 0.4 sample and $\tau_{max}=10$ sample. It is apparent that the ISI so induced, degrades the performance of coded single carrier in terms of the required SNR, for example, of about 10 dB at BER=10^{-2} in 16-QAM system. However, the transition to 64-QAM or 16-DPSK results in an irreducible error floor, even over smaller delay spread.

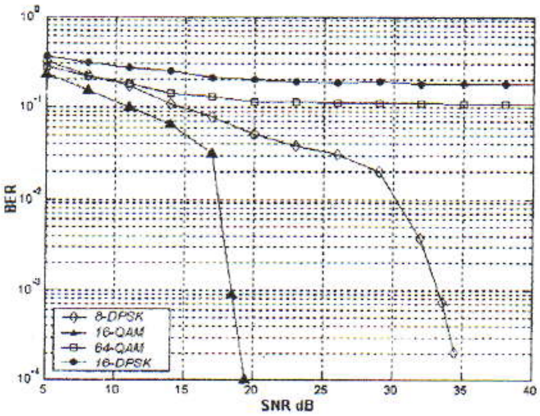

Figure (6): BER performance of single carrier system with RS (255,239) code in Rician channel of τ_{MED} 0.4 sample

Various studies have been carried out to deal with optimization of the structure of RS codes using binary modulation. Figure (7) graphed the decoder output BER versus channel SNR for two different t values 10 and 40 and fixed n=255 RS code over Rician channel of τ_{max}=30 sample and τ_{MED}=2.5 sample. Recall that the relation between code redundancy and t is $n-k=2t$. The error rates are related to the code error correction capability, because the channel generates errors randomly with numbers might exceed t within some of the messages. This effect gets more obvious for lower t.

Dashed line in the figure is conducted for 20-error correction capability with 127-code length, where lower error rates are resulted under the same channel condition. Because of that a longer code word is more susceptible to random channel errors. The encoding process, to ensure enough error protection against channel degradation, is based on a mother code. In order to guarantee more system flexibility a shortening procedure is inserted, as shown in figure (8). RS (245,235) and (230,220) shortened code performs better than the mother RS code (255,245) by a maximum of 3dB in channel SNR to achieve the error-free reception.

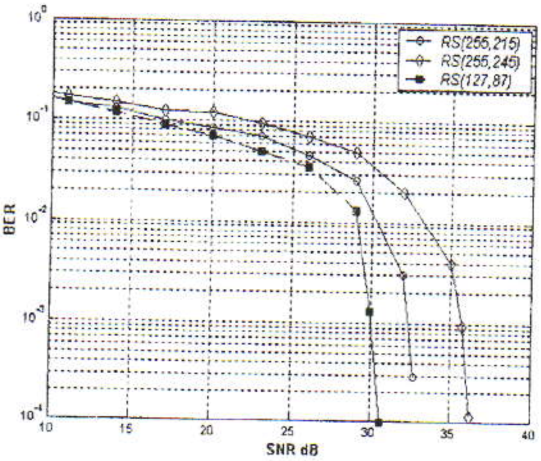

Figure (7): BER performance comparison of coded 16-QAM signal at different t values over Rician channel of τ_{max}=30 sample.

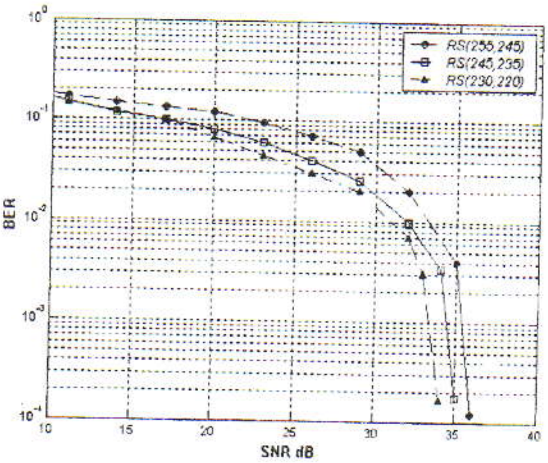

Figure (8): BER performance comparison of different RS coded 16-QAM signal over Rician channel of τ_{max}=30 sample.

IX. Conclusions

From the simulated error rates of RS coded single carrier system over AWGN channel using QAM and DPSK modulated types, it is found that QAM signal performance is better than of DPSK signal by about 12dB for 64-point constellation size. Also, 16-QAM coded signal over fading channel exhibits a more robust performance than DPSK even of lower order constellation.

Lower error rates can be achieved using more error code correction capability and/or shorter code word since it is less susceptible to random channel errors.

References

[1] M. J. Riley and E. G. Richardson, " Digital Video Communications", ARTECH HOUSE, INC. 1997.

[2] Y. Xu AND T. Zhang, " Variable Shortened-and-Punctured Reed-Solomon Codes for Packet Loss Protection", IEEE Transactions on Broadcasting, Vol. 48, No. 3, pp. 237-244, September 2002.

[3] R. Blahut, "Theory and Practice of Error Control Codes", Reading, MA: Addison-Wasely, 1985.

[4] U. Reimers, "Digital Video Broadcasting (DVB); The international standard for Digital Televsion",

Springer-verlag Berlin Heidelerge, Newyork, 2001.

Appendix A

Decoding is carried out by checking whether the received sequence is a code word, i.e., if $r.\ p^T=0$, and correcting the error by evaluating the syndrome at the receiver as

$$S = r\,.\,P^T = (c+e).\,P^T$$
$$S = c.\,P^T + e.\,P^T$$
$$S = e.\,P^T \qquad (A.1)$$

this equation can be solved to obtain e and identify the position and the value of the error. Suppose there are v errors in positions i_1, i_2, ..., i_v whose error magnitudes are e_{il}, $l=1,2,...,v$ respectively, and given by the error polynomial:

$$e(x) = e_{i1}x^{i1} + e_{i2}x^{i2} + \ldots\ldots + e_{iv}x^{iv} \qquad (A.2)$$

Then

$$\left[S_1\ S_2 \ldots S_{2t}\right] = \left[e_{i1}\ e_{i2} \ldots e_{iv}\right] \begin{pmatrix} \alpha^{i1} & \alpha^{2i1} & \ldots\ldots & \alpha^{2t\,i1} \\ \alpha^{i2} & \alpha^{2i2} & \ldots\ldots & \alpha^{2t\,i2} \\ \vdots & \vdots & & \vdots \\ \alpha^{iv} & \alpha^{2iv} & \ldots\ldots & \alpha^{2t\,i2} \end{pmatrix} \qquad (A.3)$$

or $$S = E.\ R_\alpha$$

In order to recover the original data, the error locators $\lambda_l = \alpha^{il}$, $l=1,2,...v$ must be calculated as:

$$\lambda(x) = \lambda_v x^v + \lambda_{v-1}x^{v-1} + \ldots\ldots + \lambda_1 x + 1 \qquad (A.4)$$
$$= (1-\alpha^{i1}x)(1-\alpha^{i2}x)\ldots\ldots\ldots(1-\alpha^{iv}x) \qquad (A.5)$$

the zeros of the error locator polynomial define the inverse of the error positions, for example, if $x=\alpha^{-il}$, $\lambda(\alpha^{-il})=0$ and states that an error exists at position l. By setting $x=\alpha^{-il}$, and multiplying both sides of the last equation by $e_{il}\alpha^{(j+v)il}$

$$e_{il}\alpha^{(j+v)il}[\lambda(\alpha^{-il}) = 0 = \lambda_v\alpha^{-ilv} + \lambda_{v-1}\alpha^{-il(v-1)} + \ldots + \lambda_1\alpha^{-il} + 1]$$

$$e_{il}[\lambda_v\alpha^{ilj} + \lambda_{v-1}\alpha^{il(j-1)} + \ldots + \lambda_1\alpha^{il(j+v-l)} + \alpha^{il(j+v)}] = 0 \qquad (A.6)$$

Since the equation (A.6) holds for $l=1,2,...v$, sum up these equations for all l gives an equation for each i in the form

$$\sum_{l=1}^{v} e_{i_l}\left(\lambda_v\alpha^{j.i_l} + \lambda_{v-1}\alpha^{(j+1).i_l} + \ldots\ldots + \lambda_1\alpha^{(j+v-1).i_l} + \alpha^{(j+v).i_l}\right) = 0 \qquad (A.7)$$

By separating the sum of each term, (A.7) can be rewritten as

$$\sum_{l=1}^{v} e_{i_l}\lambda_v\alpha^{j.i_l} + \sum_{l=1}^{v} e_{i_l}\lambda_{v-1}\alpha^{(j+1)i_l} + \ldots\ldots + \sum_{l=1}^{v} e_{i_l}\lambda_1\alpha^{(j+v-1)i_l} + \sum_{l=1}^{v} e_{i_l}\alpha^{(j+v)i_l} = 0 \qquad (A.8)$$

but

$$\sum_{l=1}^{v} e_{i_l}\alpha^{(j+v).i_l} = S_{j+v} \qquad (A.9)$$

Thus, (A.7) becomes as given by

$$S_j\lambda_v + S_{j+1}\lambda_{v-1} + \ldots\ldots + S_{j+v-1}\lambda_1 + S_{j+v} = 0 \qquad (A.10)$$

Since RS code can locate and correct up to $v= t$ errors, so the equation (A.10) must be satisfied for $1 \le j \le v$. For $j=1$:

$$S_1\lambda_v + S_2\lambda_{v-1} + \ldots\ldots + S_v\lambda_1 + S_{v+1} = 0 \qquad (A.11)$$

and can be arranged in matrix form as

$$\begin{pmatrix} S_1 & S_2 \ldots\ldots & S_{v-1} & S_v \end{pmatrix} \begin{pmatrix} \lambda_v \\ \lambda_{v-1} \\ \vdots \\ \lambda_1 \end{pmatrix} = - S_{v+1} \qquad (A.12)$$

by repeating these steps for $j = 2,3,v$, we produce

$$\begin{pmatrix} S_1 & S_2 & \ldots & S_{v-1} & S_v \\ S_2 & S_3 & \ldots & S_v & S_{v+1} \\ \vdots & \vdots & & \vdots & \vdots \\ S_v & S_{v+1} & \ldots & S_{2v-2} & S_{2v-1} \end{pmatrix} \begin{pmatrix} \lambda_v \\ \lambda_{v-1} \\ \vdots \\ \lambda_1 \end{pmatrix} = \begin{pmatrix} -S_{v+1} \\ -S_{v+2} \\ \vdots \\ -S_{2v} \end{pmatrix} \qquad (A.13)$$

or $$SS.\ \lambda = S_v$$

The error locator polynomial can be obtained by inverting the matrix SS as shown:

$$\lambda = SS^{-1}.\ S_v \qquad (A.14)$$

and by using the syndromes and the error locator polynomial roots, the error magnitude may be calculated from (A.3) by inverting the R_α matrix [Riley & Richardson 1997], [Blahut 1985]:

$$E = S.\ R_\alpha^{-1} \qquad (A.15)$$