International Journal of Electronics Engineering, 3 (2), 2011, pp. 299–303 © Serials Publications, ISSN : 0973-7383

Error Probability of RS Code Over Wireless Channel

Mohammad Aftab Alam Khan[1] **& Mehwash Farooqi**[1]

[1]*Department of ECE, IIMT Engineering College, Meerut, India*

E-mail: er.aftab@ymail.com, er.mehwash@ymail.com

Abstract: Reed-Solomon codes are an important class of error correcting codes used in many applications related to communications and digital storage. The fundamental operations in Reed-Solomon encoding and decoding involve Galois field arithmetic. Computer simulation tool, MATLAB is used to create and run extensively the entire simulation model for performance evaluation. It is discovered that the performance of RS codes can be assess through the function of its block size, redundancy and code rate and it is observed using Bit-Error Rate (BER) performance curve. Because RS codes work at byte level, thus it is also apparent that RS codes can perform well against burst noise. The results show that code gain with high code rate is better than that of low code rate and it is found that RS coded QAM signal performs better than the coded D-PSK signal with the same modulation size.

Keywords: Reed-Solomon Codes, RS encoder and decoder, M-PSK, Bit Error Rate.

1. INTRODUCTION

In real world communication, errors are introduced in messages sent from one point to another as shown in Figure 1. Reed-Solomon is an error-correcting coding system that was devised to address the issue of correcting multiple errors especially burst-type errors in mass storage devices (hard disk drives, DVD, barcode tags), wireless and mobile communications units, satellite links, digital TV, digital video broadcasting (DVB), and modem technologies like xDSL (“x” referring to all the existing DSL solutions, whether ADSL, VDSL, SDSL, or HDSL).

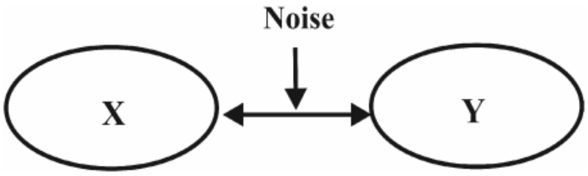

Figure 1: Two Points Exchange Information

In order for the transmitted data to be corrected in the event that it acquires errors, it has to be encoded. The receiver uses the appended encoded bits to determine and correct the errors upon reception of the transmitted signal. The number and type of errors that are correctable depend on the specific Reed-Solomon coding scheme used. A Reed-Solomon code is specified as *RS* (*n*, *k*) with s-bit symbols, where *n* is the total number of bytes the code word contains and k is the number of data bytes. The number of parity bytes is equal to *n* – *k*, where *n* is 2 raised to the power of *s* minus one (*2s –1*). A Reed-Solomon decoder can correct up to t number of bytes, where *2t* = *n* – *k*. Figure 2 shows a Reed-Solomon code word in which the data is left unaltered while the parity bits are suffixed to the data bits. This type of code is also known as a systematic code. A well-known example of a RS code is *RS (255, 223)* with 8-bit symbols. For this specific Reed-Solomon code, each code word has 255 total bytes, with 223 bytes of data and 32 bytes for parity. This code has: *n* = 255, *k* = 223, *s* = 8, *2t* = 32, *t* = 16.

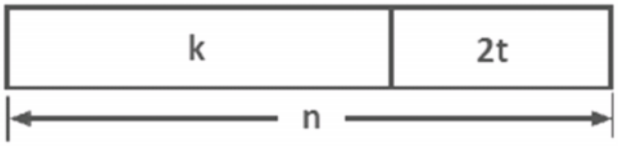

Figure 2: Reed Solomon Code Word

This means that the decoder can automatically correct 16 symbol errors up to 16 bytes anywhere in the code word.

1.1. Reed-Solomon Terminology

- Symbol Width is the number of bits per symbol
- Code Word is the block of n symbols
- *RS* (*n*, *k*) code:
  - *n* is the total number of symbols per code word
  - *k* is the number of information symbols per code word
- Code Rate is equal to *k / n*
- *r* = (*n* – *k*) is the number of check symbols.
- *t* = (*n* – *k*) */ 2* is the maximum number of Symbols with errors that can be corrected.

2. RS SYSTEM MODEL

In this subsection the testing is applied to single carrier system with (AWGN) channel model using (QAM) technique. AWGN channel is having a frequency spectrum that is continuous and uniform over a specified frequency band or it has equal power per hertz over the specified frequency band QAM is a modulation technique where its amplitude is allowed to vary with phase, also can be viewed as a combination of amplitude shift keying (ASK) as well as phase shift keying (PSK). It can be viewed as ASK in two dimension. Figure 3 demonstrates the simulation model employed by this section.

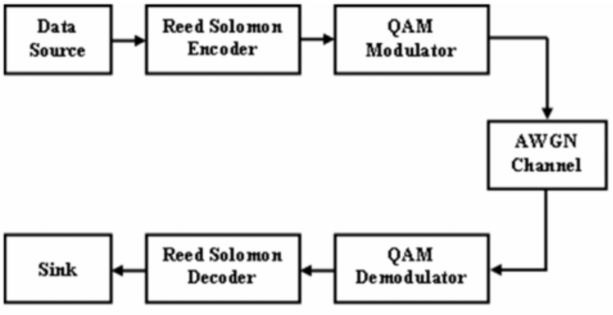

Figure 3: Single Carrier Transceiver

3. RS ENCODING & DECODING PROCESS

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 [1]. The Reed-Solomon 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 field) [2].

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 α^{136} α^{240} α^{208} α^{195} α^{181} α^{158} α^{201} α^{100} α^{11} α^{83} α^{167} α^{107} α^{113} α^{110} α^{106} α^{121}. 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.

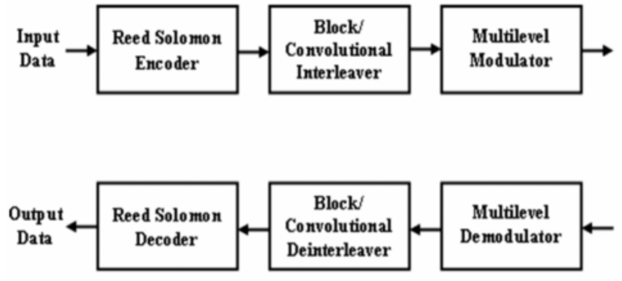

Figure 4: Block Diagram of Coded Single Carrier System Model

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.

4. RS ENCODER AND DECODER ALGORITHMS

4.1. Encoder Algorithm

Cyclic codes, such as Reed-Solomon codes, are described in numerous coding theory books [3] [4] [5]. Given a data polynomial $a(x)$ of degree $k < n$, $n = 2^m$, in Galois field *GF* (2*m*) and a code generating polynomial $g(x)$ of degree p, where $p \le n\text{-}k$ and

$$g(x) = \prod_{i=0}^{p-1}\left(x+\alpha^{i}\right),\ a(x) = \sum_{i=0}^{k} a_i x^{i} \qquad (1)$$

with α^i successive unity roots in GF (2^m) and a_i elements of the same field, the systematic encoding of $a(x)$ is given by

$$C(x) = a(x)x^{n-k} - R(x) \qquad (2)$$

where $R(x)$ is the remainder of the division $a(x)x^{n-k}$ by $g(x)$.

Given two polynomials $P(x)$ $P(x)$ and $G(x)$ with coefficients in the *GF* (2^m) field,

$$P(x) = \sum_{i=0}^{M} a_i x^{i},\ G(x) = \prod_{i=0}^{N-1} x + \alpha^{i} \qquad (3)$$

the remainder $R(x)$ of $P(x)$ divided by $G(x)$can be expressed as:

$$R(x)=\sum_{i=0}^{N-1}\beta^{(i)}\prod_{k=i}^{N-1}x+\alpha^{k} \qquad (4)$$

Where $N = n - k$, α^i are the roots of the polynomial $G(x)$, and $\beta^{(i)}$ are GF polynomials generated by successive Horner reductions of $P(x)$ by α^i. Successive Horner reductions of the polynomial by are illustrated in Table 1. [6].

The entries in the first row are the coefficients of the polynomial to be reduced and the entries in the rightmost column are the unity roots. If the remainder (j) is zero, then j is a root of $P(x)$. The entries of the second row are the coefficients of the reduced polynomial with 0, and so on. Each row represents the coefficients of the polynomial to be reduced with the root of the $g(x)$ polynomial in the corresponding position of the rightmost column. The result of the reduction is the next row.

Table 1
Horner Reduction Table

a_n	a_{n-1}	a_{n-2}	a_0	α^0
a_n	$a_n\alpha^0 {}_+ a_{n-1}$	$(a_n\alpha^0+a_{n-1})\alpha^0+a_{n-2}$	β^0	α^1
a_n	$a_n\alpha^1 {}_+ a_n\alpha^0+a_{n-1}$	$(a_n\alpha^1+a_n\alpha^0+a_{n-1})\alpha^1+$ $(a_n\alpha^0+a_{n-1})\alpha^0+a_{n-2}$		α^2
.	.	.	.	.
a_n	$\beta^{(N-1)}$	…	…	α^{N-1}

The encoding algorithm is performed as follows:

- Perform the successive Horner reductions on the polynomial $a(x)x^{n-k}$ to obtain the coefficients $\beta^{(i)}$,
- Calculate $R(x)$ as described in Equation 4,
- Calculate $C(x)$ as described in Equation 2.

4.2. Decoder Algorithm

Suppose the received code word is

$$C(x)=\sum_{i=0}^{n-1}c_i x^i \qquad (5)$$

Instead of checking the validity of the code word by encoding the data portion of the received code word and then comparing the computed parity bits to the received parity bits, the decoder starts by directly computing the syndromes of the received codeword using Equation 6.

$$S_i=C^T\sum\nolimits_i \qquad (6)$$

where C is a vector formed from the coefficients of the data polynomial and Σ_i are the syndrome vectors computed using,

$$\Sigma i=\sum_{k=0}^{2^n-1}x^k\left(\alpha^k\right)^i \qquad (7)$$

If all the syndromes are zeroes, there are no errors. If any syndrome differs from zero, the following syndrome matrix equation is solved, where λ_i are the coefficients of the error locator polynomial.

$$\begin{pmatrix} S_0 & S_1 & . & S_{\frac{N}{2}-1} \\ S_1 & S_2 & . & S_{\frac{N}{2}} \\ S_2 & S_3 & . & S_{\frac{N}{2}+1} \\ . & . & . & . \\ . & . & . & . \\ S_{\frac{N}{2}-2} & S_{\frac{N}{2}-1} & . & S_{N-1} \\ S_{\frac{N}{2}-1} & S_{\frac{N}{2}} & . & S_{N-2} \end{pmatrix}\begin{pmatrix} \lambda_{\frac{N}{2}-1} \\ \lambda_{\frac{N}{2}-2} \\ \lambda_{\frac{N}{2}-3} \\ . \\ . \\ . \\ \lambda_1 \\ \lambda_0 \end{pmatrix}=\begin{pmatrix} S_{\frac{N}{2}} \\ S_{\frac{N}{2}+1} \\ S_{\frac{N}{2}+2} \\ . \\ . \\ . \\ S_{N-2} \\ S_{N-1} \end{pmatrix} \qquad (8)$$

The above system of equations is solved using Gaussian elimination to obtain Equation 9.

$$\begin{pmatrix} 1 & \Xi_1 & . & \Xi_{\frac{N}{2}-1} \\ 0 & 1 & . & \Xi_{\frac{N}{2}} \\ 0 & 0 & . & \Xi_{\frac{N}{2}+1} \\ . & . & . & . \\ . & . & . & . \\ 0 & 0 & . & \Xi_{N-1} \\ 0 & 0 & . & 1 \end{pmatrix}\begin{pmatrix} \lambda_{\frac{N}{2}-1} \\ \lambda_{\frac{N}{2}-2} \\ \lambda_{\frac{N}{2}-3} \\ . \\ . \\ \lambda_1 \\ \lambda_0 \end{pmatrix}=\begin{pmatrix} S_{\frac{N}{2}} \\ S_{\frac{N}{2}+1} \\ S_{\frac{N}{2}+2} \\ . \\ . \\ S_{N-2} \\ S_{N-1} \end{pmatrix} \qquad (9)$$

This system of equations is then solved to produce

$$\lambda_0=\Xi_{N-1,}\lambda_1=\Xi_{N-1}\lambda_0+\Xi_{N-1}\ldots \qquad (10)$$

The error locator polynomial is solved using Chien search. The inverse of the solution of the error locator polynomial represents the position of the bit error.

5. SIMULATED 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. 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} (Mean Excess Delay) of approximately 0.4 sample and τ_{max} (Maximum Excess Delay) of 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.

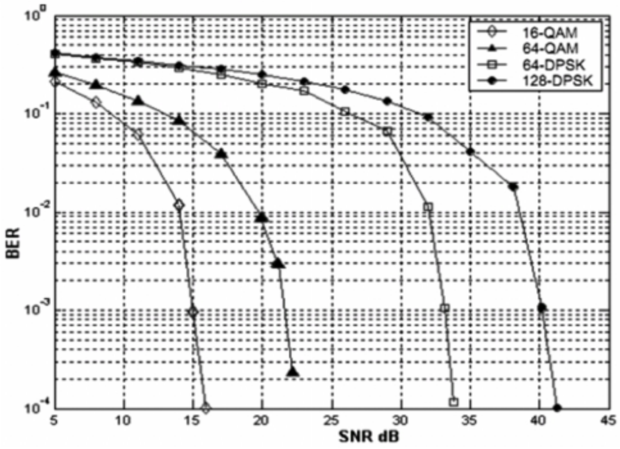

Figure 5: BER Performance of Single Carrier System in AWGN Channel with RS (255,239) Code

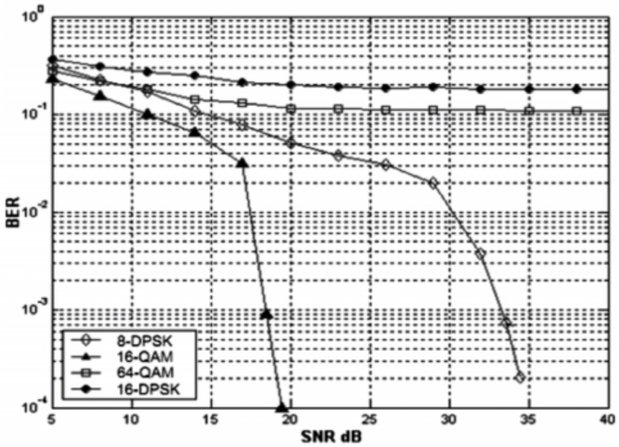

Figure 6: BER Performance of Single Carrier System with RS (255,239) Code in Rician Channel of τ_{MED} = 0.4 Sample

However, the transition to 64-QAM or 16-DPSK results in an irreducible error floor, even over smaller delay spread. Various studies have been carried out to deal with optimization of the structure of Reed-Solomon 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.

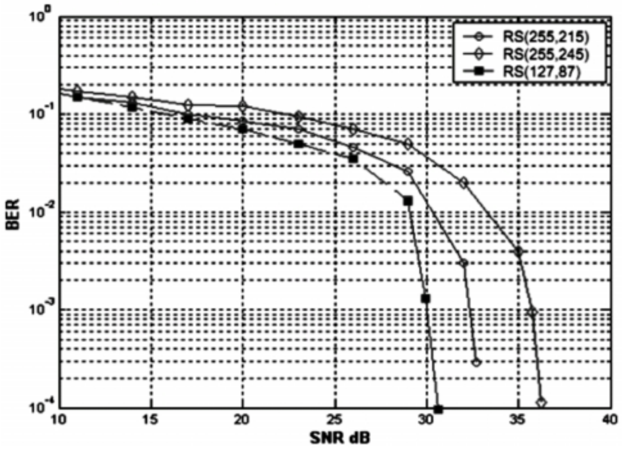

Figure 7: BER Performance Comparison of Coded 16-QAM Signal at Different t Values Over Rician Channel of τ_{max}=30 Sample

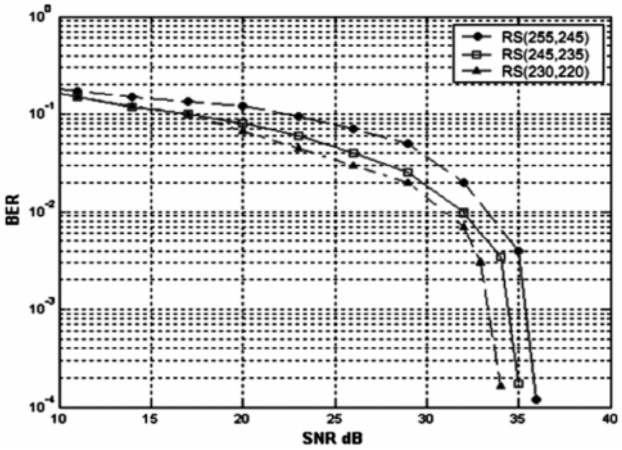

Figure 8: BER Performance Comparison of Different RS Coded 16-QAM Signal Over Rician Channel of τ_{max}=30 Sample

Recall that the relation between code redundancy and *t* is *n*-*k* = 2*t*. 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. In the figure dashed line 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.

6. CONCLUSION

From the simulated error rates of Reed-Solomon 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] E. R. Berlekamp, "Algebraic Coding Theory," Aegean Park Press, 1984.

[4] R. E. Blahut, "Algebraic Codes for Data Transmission," Cambridge University Press, 2003.

[5] S. B. Wicker, "Error Control Systems for Digital Communication and Storage," Prentice Hall Inc., 1995.

[6] C. Sidney Burrus, James W. Fox, Gary A. Sitton, and Sven Treitel, "Horner's Method for Evaluating and Deûating Polynomials," Rice University November 26, 2003.