IJCSC International Journal of Computer Science and Communication Vol. 3, No. 1, January-June 2012, pp. 37-40

A STUDY ON PERFORMANCE EVALUATION OF REED-SOLOMON (RS) CODES THROUGH AN AWGN CHANNEL MODEL IN A COMMUNICATION SYSTEM

D. Venkata Ratnam[1], S. SivaKumar[2], R. Sneha[3], N. Suresh Reddy[4], P S Brahmanandam[5*], S. Gopi Krishna[6]

[1]Dept. of ECE, K L University, Vaddeswaram 522502, India, *E-mail: ratnam20002v@gmail.com.*

[2]Dept. of ECE, K L University, Vaddeswaram 522502, India, *E-mail: kumar.siva963@gmail.com.*

[3]Dept. of ECE, K L University, Vaddeswaram 522502, India, *E-mail: sneharaavi@gmail.com.*

[4]Dept. of ECE, K L University, Vaddeswaram 522502, India, *E-mail: sureshy@rocketmail.com.*

[*5]Dept. of ECE, K L University, Vaddeswaram 522502, India, *E-mail: anand.potula@gmail.com.*

[6]Dept. of ECE, K L University, Vaddeswaram 522502, India, *E-mail: gopi.seemala@gmail.com.*

ABSTRACT

Typical communications systems use several codes that are suited for correcting different types of errors. Reed-Solomon (RS) codes are the most powerful in the family of linear block codes and are arguably the most widely used type of error control codes. This paper examines the performance evaluation of phase shift keying (PSK) technique modulation using the Reed-Solomon (RS) codes, which can be effectively used for burst error correction. This particular type of codes was used to calculate the bit error rate through an Additive White Gaussian Noise (AWGN) channel. Performances of PSK with RS codes are assessed in terms of bit rate error (BER) and signal energy to noise power density ratio (Eb/No). Simulations are carried out by writing an effective software code in MATLAB. It is found that the RS codes demonstrate best performance compared to BCH, Hamming and Cyclic codes.

Keywords: Reed-solomon codes, additive white gaussian noise channel, bose-chaudhuri-hocquenghem code, and bit rate error.

1. INTRODUCTION

Communication is the process of establishing connection or link between two points of information or a basic process of exchanging information. The electronic equipment which is used for communication purpose is called a communication system. The main aim of this system is to transmit the information bearing signal from source located at one point to a user or destination located at another point some distance away. A typical communication system is shown in Figure 1. An efficient communication system is one which can deliver the required amount of information to destination without any signal loss. Mostly, we find that the loss of data is due to fading characteristics of a channel, frequency selectivity, interference, nonlinearity or dispersion etc. The communication channel is the physical medium that is used for transmitting signals from transmitter to receiver. In wireless system, this channel consists of atmosphere, while for traditional telephony, this channel is wired; there are optical channels, under water acoustic channels etc. One can discriminate these channels on the basis of their property and characteristics, which is also same for AWGN channel. It is a channel model which can alleviate the impairments primarily due to its additive noise property. It is a type of channel with all the characteristics by which one can purge linear addition of wideband or white noise with a constant spectral density and a Gaussian distribution of amplitude.

In general, due to addition of the noise when signal is passed through AWGN channel, it gets distorted. This alters the original message bits and can become a severe problem to the accuracy and performance of the digital system. Therefore, error detecting and correcting techniques play a vital role. One way to overcome the errors in the transmission is by maximizing the ratio Eb/No. But, in practice the ratio can not be increased beyond the limit.

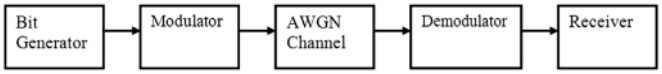

Figure 1: Depicts Typical Communication System with AWGN Channel.

Higher constellation modulation techniques are needed for effectively mitigating the impairments of a multi-path fading channel along with a high data rates in a limited bandwidth. Vishakan Ponampalam et al. [1, 2] explained that there are several types of modulation for phase shift keying technique like BPSK and QPSK. For BPSK, there are phase ambiguity problems at the receiver. To resolve these problems, differentially encoded QPSK is used more often in practice [3]. On the other hand, Jorge and Patrick [4] propose the higher constellation to avoid the degradation of BER.

In this paper, RS coding techniques are tested with simulations for improving the reliability and the quality of the transmitted signal. On the other hand, it is possible to reduce Eb/No for a fixed BER, which can also reduce the transmitted power and size of the antenna.

2. CODING TECHNIQUES

In order to achieve better performance, high constellation modulation techniques of PSK including BPSK and QPSK are chosen. BPSK in the presence of noise can perform better and yields the minimum value of probability of error, in which the original signal will be squared at the receiver end. So, even the original signal has changed its sign, the recovered signal however left unchanged. To mitigate this problem, QPSK technique has been considered. In QPSK for the same BER, bandwidth required is reduced to half compared to BPSK. Due to this, data transmission rate of QPSK is enlarged. To lessen BER further, error correcting codes like Hamming, Cyclic, BCH and RS codes etc. are introduced in the communication system. Due to inability of correcting random and burst errors, Hamming and Cyclic codes are considered as inefficient.

2.1. BCH CODES

The BCH codes form a large class of powerful random error-correcting Cyclic codes. This class of codes is a remarkable generalization of the Hamming codes for multiple-error correction. Binary BCH codes were discovered by Hocquenghem in 1959 and independently by Bose and Chaudhuri in 1960.

For any positive integers $m(m \geq 3)$ and $t(t < 2m - 1)$, there exists a binary BCH code with the following parameters:

Block length	:	$n = 2^m - 1$
Number of parity check bits	:	$n - k <= mt$
Minimum distance	:	$dmin >= 2t + 1$

Clearly, this code is capable of correcting any combination of t or fewer errors in a block of $n = 2^m - 1$ digits. It is called as a t-error-correcting BCH code.

The generator polynomial of this code is specified in terms of its roots from the Galois field GF (2^m). Let A be a primitive element in GF (2^m).

The generator polynomial $g(X)$ of the t-error correcting BCH code of length $2^m - 1$ is the lowest-degree polynomial over GF(2) which has

$$A^1, A^2, A^3 ..... A^{2t} \quad (1)$$

As its roots [i.e., $g(i) = 0$ for $1 \leq i \leq 2t$. It follows that $g(X)$ has $A^1, A^2, A^3 ..... A^{2t}$ and their conjugates as all its roots. Let $mi(X)$ be the minimal polynomial of $g(X)$. Then $g(X)$ must be the least common multiple (LCM) of $m^1(X)$, $m^2(X)$,.... $m^{2t}(X)$ that is,

$$g(X) = \{\text{LCM}(m^1(X),.....,m^{2t}(X))\} \quad (2)$$

The generator polynomial $g(X)$ of the binary t-error correcting BCH code of length 2^{m-1} given by (2) can be reduced to

$$g(X) = \{\text{LCM}(m^1(X), m^2(X) , ... m^{2t-1}(X)\} \quad (3)$$

Since the degree of each minimal polynomial is m or less, the degree of $g(X)$ is at most mt. That is, the number of parity check digits, $n - k$, of the code is at most equal to mt. There is no simple formula for enumerating $n - k$, but if t is small, $n - k$ is exactly equal to mt minimum distance of this code is exactly 7. BCH codes have a very good efficiency but are only useful when we require a code with small distance. BCH codes are only useful when $D <= n/\log n$. In practical, errors occur often as burst and in this case severe data loss can occur. R-S codes, a powerful class of non binary block codes, particularly useful for correcting burst errors effected bits that correspond to a much smaller number of elements in the field on which the RS codes are defined. For example, if a binary code constructed from the RSF256 [256; 230] code is encountered with 30 consecutive errors, these errors affect utmost 5 elements in the field F256 and this error can easily be corrected.

2.2. REED-SOLOMON CODES

In 1960, Irving Reed and Gus Solomon published a paper in the Journal of the Society for Industrial and Applied Mathematics [5] on polynomial codes over finite elements. RS codes are the codes with symbols from the Galois field $GF(q)$, where q is any power of p, which is a prime number. The special subclass of q-ary BCH codes for which $s = 1$ is the most important subclass of q-ary BCH codes. The codes of this subclass are usually called the Reed-Solomon codes in honor of their discoverers.

A t-error correcting Reed-Solomon code with symbols from $GF(q)$ has the following parameters:

Block length	:	$n = q-1$
Number of parity check bits	:	$n - k = 2t$
Minimum distance	:	$dmin = 2t + 1$

We consider Reed-Solomon codes with code symbols from the Galois field $GF(2m)$ (i.e., $q = 2m$). Let be a primitive element in $GF(2m)$.

The generator polynomial of a primitive t-error correcting Reed-Solomon code of length $2^m - 1$ is

$$g(X) = (X + A)(X + A^2) ..... (X + A^{2t})$$

$$= g0 + g1X + g2X^2 + ... + g2t-1\ X^{2t-1} + X^2 \quad (4)$$

The code generated by $g(X)$ is an $(n, n - 2t)$ Cyclic code which consists of those polynomials of degree $n - 1$ or less with coefficients from $GF(2^m)$ that are multiples of $g(X)$. Encoding of this code is similar to the binary case.

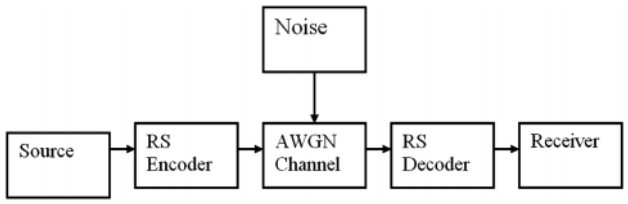

Figure 2: Shows the Block Diagram of Communication System with RS Code.

Figure 2 describes the basic elements of RC codes in a typical communication system through AWGN channel. Although many new codes are introduced, still these codes continue to be used in many applications. Most notably, they are extensively used in storage devices like CDs, DVDs, and hard-drives due to their capability of correcting burst errors. These codes became more popular as they were optimal codes. Since coding efficiency increases with the code length, RS codes have a special attraction. They can be configured with long block lengths (in bits) with less decoding time than other codes of similar lengths. This is because the decoder logic works with symbol-based rather than bit-based arithmetic. Hence, for 8-bit symbols, the arithmetic operations would all be at the byte level. This increases the complexity of the logic, compared with binary codes of the same length, but it also increases the throughput.

2.2.1. Need For RS-Codes

RS codes attain the major possible code minimum distance for any linear code with the unchanged encoder and output lengths. The distance between two code words is definite as the number of symbols in which the sequences differ.

For RS, the code minimum distance is

$$dmin = N - K + 1 \quad (5)$$

RS codes have a significant property that they are capable of correcting any set of N-k symbols within the block. They can be designed to have any redundancy. The complexity of high speed performance increases with redundancy. RS codes have high code rates. RS codes are effective for the channels that have memory. Two information symbols can be additional to RS code length N without reducing its minimum distance.

3. RESULTS AND DISCUSSION

The simulations are carried out for BPSK and QPSK. The simulation programs are developed in MATLAB 2009a version. The value of (Eb/No) in AWGN channel is varied from 0(dB) to 10(dB) in order to observe the performance of BER. The comparison results are divided in to four parts. The details are as follows.

(*i*) without block codes.

(*ii*) Hamming and Cyclic codes.

(*iii*) Hamming, Cyclic and BCH codes.

(*iv*) BCH and RS codes.

Figures 3 and 4 show BER results of BPSK and QPSK communication system without block codes. It can be seen from these figures that BER decreases as Eb/No increases. Hamming encoder and decoder options are used in MATLAB program. The Hamming encoder block creates a Hamming code with message length k and codeword length n. The number n must have the form $2M - 1$, where M is an integer greater than or equal to 3. Then, k equals $N - M$. Generator must be the same as the value of the massage length (k) in Hamming encoder [1]. Figure 5 shows BER results with Cyclic and hamming codes.

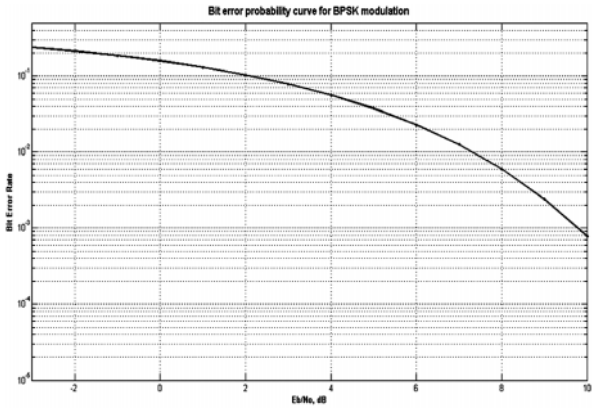

Figure 3: Shows BER vs. (Eb/No) of a Communication Syste (using BPSK) without Error Correcting Codes.

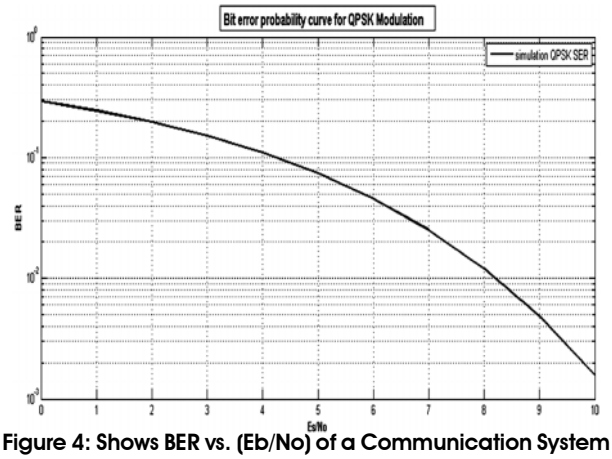

Figure 4: Shows BER vs. (Eb/No) of a Communication System (using QPSK) without Error Correcting Codes.

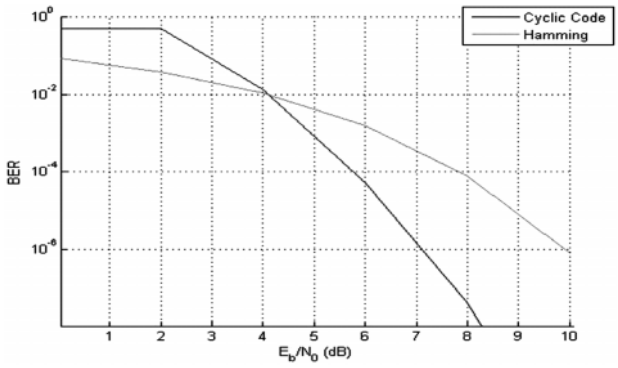

Figure 5: Shows BER vs. (Eb/No) of a Communication System with Cyclic and Hamming Codes.

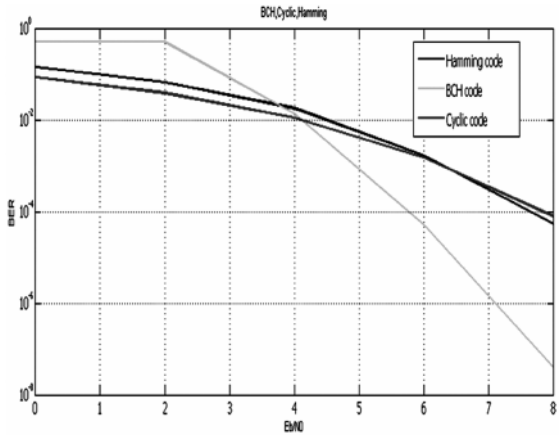

Figure 6: Shows BER vs. (Eb/No) of a Communication System with Cyclic, Hamming and BCH Codes.

BCH encoder and decoder codes are simulated by using MATLAB software. The BCH encoder generates a BCH code with message length k and codeword length n. The input must contain exactly k elements. The output is a vector of length n. For a given codeword length n, only specific message lengths k are valid for a BCH code. From the graph which is shown in Figure 6, the results demonstrate that the BPSK using BCH has the lowest BER compared to others. The results of Figure 7 show that the best performance occurs when the communication system uses a BCH code with $N = 31$, $K = 11$ and $t = 5$ with BPSK modulator/demodulator. In general, the BCH codes are better than Hamming and Cyclic codes. It is mainly due to Hamming and Cyclic codes are capable of detecting and correcting single errors only whereas BCH codes are capable of detecting and correcting multiple errors.

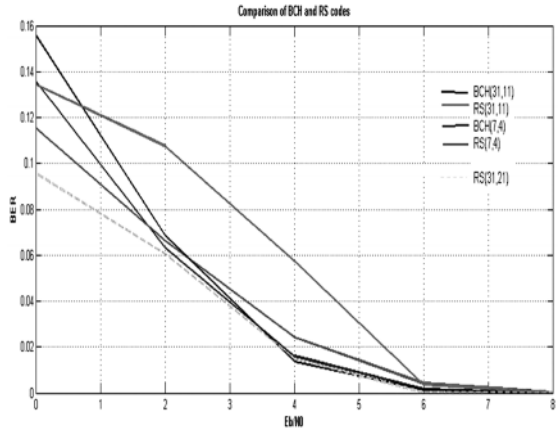

Figure 7: Shows BER vs. (Eb/No) of a Communication System with BCH and RS Codes.

Better performance is obtained for RS codes by choosing $n = 31$ and $k = 21$ as it can be seen from Figure 7. Hence, RS codes can be used to correct more number of errors (burst errors), since its BER is low.

4. CONCLUSIONS

In this paper, Reed-Solomon codes are implemented for communication systems using BPSK and QPSK through AWGN channel. RS codes come under a powerful class of non-binary block codes, which are particularly useful for correcting burst errors. It is observed that best performance occurs when communication systems use an RS code with $n = 31$ and $k = 21$ with BPSK/QPSK modulator or demodulator. It can, therefore, conclude that the approach presented in this research will be immensely useful for robust error correction detection in communication systems.

REFERENCES

[1] Suzi Seroja Sarnin, Nani Fadzlina Naim, Wan Nor Syafizan W. Muhamad, "Performance Evaluation of Phase Shift Keying Modulation Technique using BCH Code, Cyclic Code and Hamming Code Through AWGN Channel Model in Communication System", *Information Sciences and Intraction Sciences (ICIS)*, 2010, 3rd international conference, 03 Aug 2010.

[2] Vishakan Ponnampalam, Branka Vucetic, "Maximum Likelihood Decoding of Reed Solomon Codes", *ISIT* 1998, Cambridge MA, USA, August 16-August 21.

[3] MacWilliams, F. J. and Sloane, N. J. A., "The Theory of Error-Correcting Codes", Amsterdam, Netherlands: North-Holland, 1977.

[4] Jorge Castineira Moreira and Patrick Guy Farrell, "Essentials of Error Control Coding", Argentina: Wiley and Son, 2006.

[5] Reed, I. S. and Solomon, G., "Polynomial Codes Over Certain Finite Fields", *SIAM Journal of Applied Math.*, **8**, 1960, pp. 300-304.

[6] Marvin K. Simon, William C Lindsey, Sami M Hinedi, "Digital Communication Techniques: Signal Design and Detection", Prentice Hall PTR, 1994.

[7] Sanjay Sharma, "Digital Communications", 4th Edition, S.K. Kataria & sons, 2009.

[8] Bernard Sklar, "Introduction to Reed Solomon Codes", *Digital Communications: Fundamentals and Applications*, 2nd Edition, Prentice Hall, 2001.