International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Reed-Solomon Galois Field Generator Polynomial Block length Bit Error Rate Signal Noise Ratio

D.Ramesh[1]; D.Vasanthalaxmi[2]& Boggarapu Kantha Rao[3]

[1]Associate Professor ECE Dept. Medha Institute of Science and Technology for Women, Khammam
dasariramesh1985@gmail.com

[2]M-Tech ECE Department, Medha Institute of Science and Technology for Women

[3]HOD &Assoc Prof, Medha Institute of Science and Technology for Women
kantharao.b@gmail.com.

Abstract

In the present world, communication system which includes wireless, satellite and space communication, reducing error is being critical. During message transferring the data might get corrupted, so high bit error rate of the wireless communication system requires employing to sundry coding methods for transferring the data. Channel coding for detection and rectification of error avails the communication systems design to reduce the noise effect during transmission. The purport of this paper is to study and analyze the performance and efficiency of Reed-Solomon (RS) Codes. In coding theory, Reed-Solomon (RS) codes are the subset of BCH codes that are one of the most potent kenned classes of linear cyclic block codes. Reed-Solomon (RS) codes are very efficient and best for rectification of burst errors and have a wide range of applications in digital communication and data storage. Reed-Solomon (RS) is the most potent technique utilized for error detection and rectification at present.

Keywords: Reed-Solomon (RS); Galois Field (GS); Generator Polynomial g(x); Block length; Bit Error Rate (BER); Signal Noise Ratio (SNR).

1. Introduction

Channel coding is a consequential signal processing operation for the efficient transmission of digital information over the channel. In channel coding the number of symbols in the source encoded message is incremented in a controlled manner in order to facilitate two fundamental objectives at the receiver one is Error detection and other is error rectification. Error detection and error rectification to achieve good communication is withal employed in contrivances. It is utilized to reduce the caliber of noise and interferences in electronic medium. The amount of error detection and rectification required and its efficacy depends on the signal to noise ratio (SNR) [1]. A channel code is a broadly used term mostly referring to the forward error rectification code. Forward error rectification (FEC) is a system of error control for data transmission, whereby the sender integrates redundant data to its messages, additionally kenned as an error rectification code. This sanctions the receiver to detect and redress errors without the desideratum to ask the sender for adscititious data. FEC is applied where retransmissions are relatively

costly or infeasible. FEC information is conventionally integrated to most mass storage contrivances to bulwark against damage to the stored data [2]. There are many types of block codes, but the most eminent is Reed Solomon coding, Golay, BCH, Multidimensional parity, and hamming codes are other example of block codes. Reed Solomon is an error-rectifying coding system that was devised to address the issue of redressing multiple errors – especially burst-type errors in mass storage contrivances (hard disk drives, DVD, barcode tags), wireless and mobile communications units, satellite links, digital TV, digital video broadcasting (DVB), and modem technologies like xDSL [3].

Reed-Solomon codes are a consequential subset of non-binary cyclic error redressing code and are the most widely used codes in practice. These codes are utilized in wide range of applications in digital communications and data storage. Reed Solomon describes a systematic way of building codes that could detect and redress multiple arbitrary symbol errors. By integrating t check symbols to the data, an RS code can detect any cumulation of up to t erroneous symbols, or correct up to ⌊t/2⌋ symbols. Furthermore, RS codes are opportune as multiple-burst bit-error rectifying codes, since a sequence of b + 1 consecutive bit errors can affect at most two symbols of size b. The cull of t is up to the designer of the code, and may be culled within wide limits.

Example:

A popular Reed Solomon code is RS (255,223) with 8-bit symbols. Each codeword contains 255 code word bytes, of which 223 bytes are data and 32 bytes are parity for this code

n = 255, k = 223, s = 8

2t = 32, t = 16

The decoder can correct any 16 symbol errors in the code word: i.e. errors in up to 16 bytes anywhere in the codeword can be automatically corrected.

Given a symbol size s, the maximum codeword length (n) for a Reed Solomon code is n = **2s – 1.** For example, the maximum length of a code with 8-bit symbols (s=8) is 255 bytes.

Reed Solomon codes may be shortened by (conceptually) making a number of data symbols zero at the encoder, not transmitting them, and then re-inserting them at the decoder. RS are block codes and are represented as RS (n, k), where n is the size of code word length and k is the number data symbols, n – k = 2t is the number of parity symbols as shown in Fig. 1.

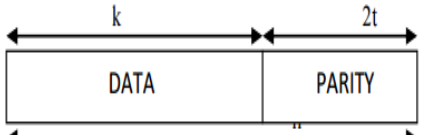

Fig. 1 Structure of RS codeword

Each symbol at input is composed of m bits given by relation n = qm -1. The message is divided into k symbols and 2t parity symbols are added to give n symbols of RS code. Reed Solomon codes are constructed using generator polynomial which is given by equation:

$g(x) = (x - \alpha^{i})(x - \alpha^{i+1}) \ldots\ldots (x - \alpha^{2t+i-1})(x - \alpha^{2t+i})$

RS encoding is based on addition operation and multiplication operation over Galois field (GF (2^m)). For GF (2^m) field m XOR gates will be required for the realization of addition operation and operation of multiplication requires m2 AND gates & m^2 -1 XOR gates using conventional approaches [4].

2. Related Work

2.1 Properties of reed Solomon codes:

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

The properties of Reed-Solomon codes make them especially suited to the applications where burst error occurs. This is because:-

It does not matter to the code how many bits in a symbol are incorrect, if multiple bits in a symbol are corrupted it only counts as a single error. Alternatively, if a data stream is not characterized by error bursts or drop-outs but by random single bit errors, a Reed-Solomon code is usually a poor choice. More effective codes are Available for this case.

- Designers are not required to use the natural sizes of Reed-Solomon code blocks. A technique known as "shortening" produces a smaller code of any desired size from a larger code. For example, the widely used (255,251) code can be converted to a (160,128). At the decoder, the same portion of the block is loaded locally with binary zeroes [5].
- A Reed–Solomon code operating on 8-bits symbols has $n = 2^8 - 1 = 255$ symbols per block because the number of symbol in the encoded block is $n = 2^m - 1$.
- For the designer its capability to correct both burst errors makes it the best choice to use as the encoding and decoding tool.

2.2 Reed-Solomon encoder:

The Reed Solomon encoder reads in k data symbols computes the n – k symbols, append the parity symbols to the k data symbols for a total of n symbols. The encoder is essentially a 2t tap shift register where each register is m bits wide. The multiplier coefficients are the coefficients of the RS engenderer polynomial. The general conception is the construction of a polynomial, the coefficient engendered will be symbols such that the engenderer polynomial will precisely divide the data/parity polynomial. From the architectural perspective, the encoder represents the set of shift registers, joined by denotes of integrators and multipliers, operating according to the rules of Galois arithmetic. The shift register represents the sequence of recollection cells, called bits, each of which contains one element of a Galois field GF(q). The symbol, contained in a categorical position, is transmitted to the output line as it leaves this position. Simultaneously, the symbol from the input line is loaded into position. Supersession of symbols takes place discretely, at rigorously defined time intervals, kenned as clocks. In hardware implementation of the shift register, its elements can be connected both sequential and in parallel manner. In sequential connection, the sending of a single m-bit symbol requires m clocks, while parallel connection requires only one clock [6].

The generator polynomial of the RS encoder is represented by

$$\mathbf{g(x) = g_0 + g_0\, x + g_0\, x^{2} + \ldots + g_{2t-1}\, x^{2t-1} + x_{2t}}$$

The hardware implementation of this RS encoder is shown in Fig. 2.

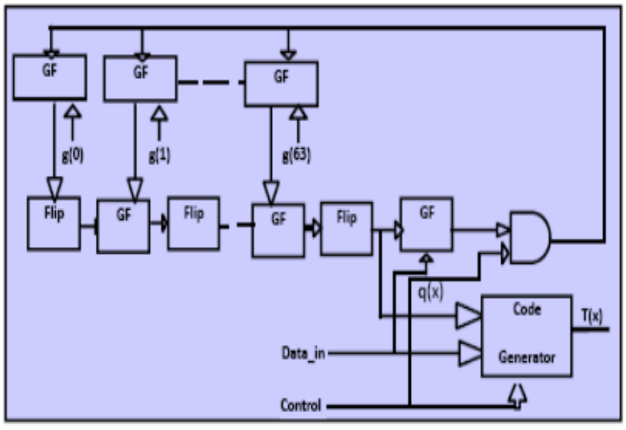

Fig 2: Block Diagram of RS Encoder.

Reed Solomon codes are based on a special area of mathematics known as Galois fields or finite fields. Finite field has the property that arithmetic operations (+, -, x, / etc.) on field elements always have a result inside the field. The basic principle of encoding is to find the remainder for the message divided by a generator

polynomial G(x). The encoder working is by simulating a linear feedback shift register with degree as G(x) is having, and feedback taps with the coefficients of the generating polynomial of the cods [7].

2.3 Reed-Solomon decoder:

The Reed Solomon decoder tries to correct errors and/or erasures by calculating the syndromes for each codeword. Based upon the syndromes the decoder is able to determine the number of errors in the received block. If there are errors present, the decoder tries to find the locations of the errors using the Berlekamp-massey algorithm by creating an error locator polynomial. The roots of this polynomial are found using the Chien search algorithm.

Using Forney's algorithm, the symbol error values are found and corrected. For an RS (n, k) code where n - k = 2T, the decoder can correct up to T symbol errors in the code word. Given that errors may only be corrected in units of single symbols (typically 8 data bits), Reed Solomon coders work best for correcting burst errors.

Decoding of Reed-Solomon codes is a complex problem that results in a bulky and extremely complicated code which requires that the developer should have an extensive knowledge in many areas of higher mathematics. A typical decoding is known as auto-regressive spectral decoding method, with following steps:-

1. Determining error syndrome (syndrome generator).
2. Building an error polynomial, carried out by using Barlekamp algorithms which are hard to implement or use some simple algorithm like Euclid's algorithm.
3. Finding the roots of this polynomial, this is usually carried out by Chein search algorithm.
4. Determining the error type, this is calculated by Forney s algorithm or any other algorithm of matrix inversion.
5. Correcting erroneous symbols by means of superimposing the mask and data word and the sequentially inverting all bits that are corrupted via XOR operation as shown in Fig. 3 [6].

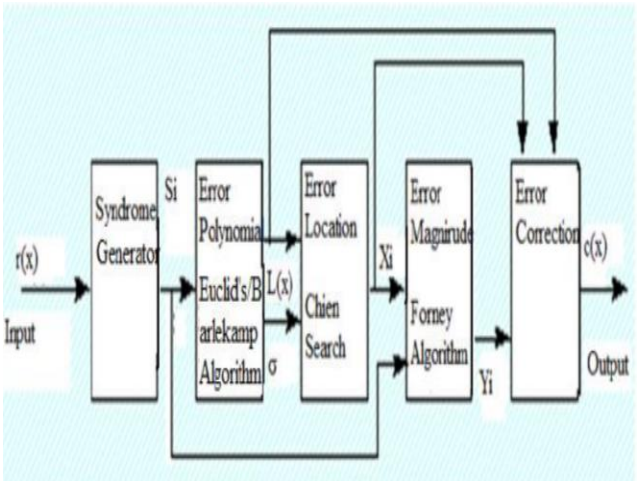

Fig 3: Block diagram of RS Decoder.

3. Implementation

Applications of reed-Solomon codes:

Data Storage: -

Reed-Solomon is very widely used in mass storage systems to correct burst errors associated with media defects. Special properties of Reed-Solomon codes make the sound quality of the CD as impressive as it is. Reed-Solomon is a main component of CD Compact Disc. In CD a scheme known as Cross-Interleaved Reed Solomon Coding (CIRC) is used. The result of CIRC is that it can correct up to 4000 bits error bursts, or about 2.5 mm on the surface of the disc [8].

Bar Code: -

All the two dimensional bar codes such as PDF-417, Maxi Code, Data matrix, QR Code, and Aztec Code use ReedSolomon error correction to allow the correct reading even if some portions of bar code are damaged. When the bar code symbol is not recognized by the bar code scanner it will treat it as an erasure. Reed-Solomon is less common in one-dimensional bar codes [5].

Satellite Broadcasting: -

The demand for satellite transponder bandwidth continues to grow, fueled by the desire to deliver television including new channels High Definition TV and IP data. BPSK coupled with traditional Reed-Solomon and Viterbi codes have been used for nearly 20 years for delivery of digital satellite TV [9].

Spread-Spectrum Systems: -

Reed-Solomon codes can be used in designing the hopping sequences. If these sequences are carefully selected, the interference caused by the other users in a multiple access environment can be greatly reduced [10].

Error Control for Systems with Feedback: -

Wicker and Bartz examined various means for using Reed-Solomon codes in applications that allow transmission of information from receiver to the transmitter. These applications include mobile data transmission systems and high reliability military communication systems [11].

Ultra Wideband (UWB): -

UWB is a wireless technology for transmitting the digital data at very high rates over a wide spectrum of frequency by using very low power. It makes it possible to transmit data at rate over 100Mbps within 10 meters. To preserve the important header information, MB-OFDM UWB adopts Reed-Solomon (23, 17) code. In receiver, RS decoder needs high speed and low latency and for this efficient hardware is used [12].

Reed-Solomon error probability:

Reed-Solomon codes are mainly used in correcting the burst errors. However it has its own error correcting capability. So, error probability is useful in saving our time for detecting and correcting the error. Let us assume an example that the code can correct 4 error symbols in an (255, 251) RS code. A maximum of 32 bits error can be corrected. So, during decoding if the decoder calculates more than 32 bits of error while performing syndrome calculation part, then send a signal that decoder cannot correct this error. Therefore plotting of the bit error probability (P) against the SNR will help. There can be a range of SNR for error to be corrected.

However range includes many parts like percentage of probability that the signal will detect. Fig. 4 shows plot between SNR and bit error probability. The code is for random 255 symbols where each symbol consists of 8 bits to be transmitted. These 255 symbols form a code word and there are 500 such codewords. However the range estimation can be calculated for different capability of correcting errors [10].

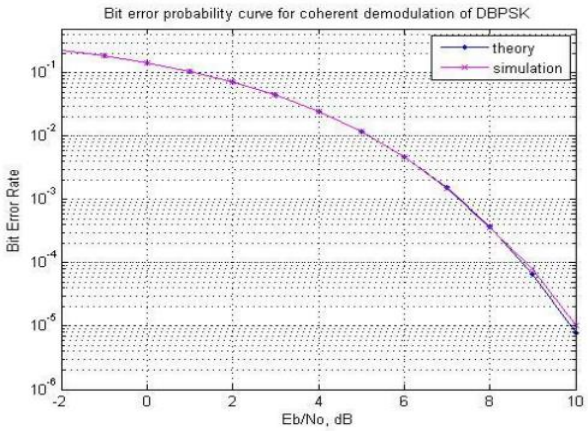

Fig 4: Graph between BER and SNR.

Analysis of the error probability graph, 255 symbols corresponds to m = 8, therefore symbol with contain 8 bits each and for different range of deduced SNR different error correcting capabilities. So different number of error bits can be found out from the plotted graph for different error capabilities. For example for 2t = 4; t = 2 therefore 16 error bits can be corrected at max. So a range of SNR can be found out using the plotted graph. Similarly for 2t = 8; t = 4 so at max 32 bits can be corrected. This range is quite bigger the previous range of SNR. This analysis helps us to find out that the decoder can correct the received signal or not and this saves a lot of time and efforts.

4. Conclusion

This paper presents clear understanding of Reed-Solomon codes utilized in error detection and rectification. RS are very potent non-binary cyclic codes and are utilized mainly for burst errors. There are different applications of REEDSolomon codes such as data storage, satellite transmission, bar code etc. and the main component of a Compact Disc is RS code. The main purport of this paper was to study the Reed-Solomon code encoding and decoding process and alsothe error probability for the RS code. The encoding process and the block diagram have been discussed and additionally the different step for decoding process has been discussed. The error probability for RS code shows that the BER performance withal amends for immensely colossal block length and shows a poor BER performance for lower SNR as the SNR value increases the curve becomes steeper.

5. References

[1] Carl Eklund, et.al. "WirelessMAN: Inside the IEEE 802.16 Standard for Wireless Metropolitan Area Networks," IEEE Press, 2006.

[2] Hagenauer, J., and Lutz, E., "Forward Error Correction Coding for Fading Compensation in Mobile Satellite Channels," IEEE JSAC, vol. SAC -5, no. 2, Feb 1987, pp. 215 -225.

[3] High-speed VLSI Architecture for Parallel Reed-Solomon Decoder", IEEE Trans. On VLSI, April 2003

[4] J. Jittawutipoka, J. Ngarmnil, "Low complexity Reed Solomon encoder using Globally optimized finite field multipliers" , IEEE Region 10 conference, Nov. 2004.

[5] www.wikipedia.org

[6] flylib.com/books/en/1.443.1.19/1/ a document on Reed-Solomon

[7] H.M. Shao, T.K. Truong, L.J. Deutsch, J. Yuen and LS. Reed, "A VLSI Design of a pipeline Reed-Solomon Decoder", IEEE Trans. Comput., vol. C-34, no. 5, pp 393-403, May 1985.

[8] Wicker, Stephen B., Bhargava, Vijay K, "Reed-Solomon Codes and the Compact Disc", IEEE Press ISBN 978-0- 7803-1025-4.

[9] J.L. Massey, "Deep Space Communications and Coding: A Match Made in Heaven," in Advanced Methods for Satellite and Deep Space Communications, Lecture Notes in Control and Information Sciences, Volume 182, Berlin: Springer-Verlag, 1992.

[10] Sanjeev Kumar, Rajni Gupta, "Bit Error Analysis of Reed-Solomon Code for Efficient Communication System," International Journal

of computer Applications (0975 – 8887) Volume 30- No. 12, September 2011.

[11] V.K Agrawal, Pankaj Goel, Gaurav Mittal, "Review of Reed-Solomon Code for Error Detection and correction," International Journal of Research in IT, Management and Engineering IJRIME Volume2, Issue6 (june-2012) ISSN: 2249-1619.

[12] Sung-woo Choi, sang-Sung Choi, Han-ho Lee, "RS decoder architecture for UWB", wireless home Network Research Team, ETRI ICACT, Feb 2006

Authors Profiles

Mr.D.RAMESH

D. Ramesh received the B.Tech. Degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2006 and M.Tech in Systems and Signal Processing from Jawaharlal Nehru Technological University, Hyderabad in 2011, is a faculty member in the department of Electronics and Communication Engineering, Medha Institute of Science and Technology for Women, Khammam and presently working as Associate Professor. His research interests include VLSI, Signal processing, Antennas. Email id dasariramesh1985@gmail.com

D.Vasanthalaxmi

M-Tech ECE Department, Medha Institute of Science and Technology for Women

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 10
June 2016

Boggarapu Kantha Rao

HOD &Assoc Prof, Medha Institute of Scienceand Technology for Women, India,B.KANTHA RAO received the B.Tech. Degree in Electronics and Communication Engineering from Jawaharlal Nehru Technological University, Hyderabad in 2006 and M.Tech in EMBEDDED SYSTEMS from Jawaharlal Nehru Technological University, Hyderabad in 2010, is a faculty member in the department of Electronics and Communication Engineering, Medha Institute of Science and Technology for Women, Khammam and presently working as Associate Professor. His research interests include Embedded systems, VLSI Design. E-mail: kantharao.b@gmail.com.