

Bit Error Rate Analysis of Reed-Solomon Code for Efficient Communication System

Sanjeev Kumar

Asst. Professor/ ECE

Amritsar college of Engg. & Technology,
Amritsar, 143001, India

Ragini Gupta

M.Tech Scholar/ECE

Amritsar college of Engg. & Technology,
Amritsar, 143001, India

ABSTRACT

In wireless, satellite, and space communication systems, reducing error is critical. High bit error rates of the wireless communication system require employing various coding methods on the data transferred. Channel coding for error detection and correction helps the communication system designers to reduce the effects of a noisy transmission channel. The purpose of this paper is to study and investigate the performance of Reed-Solomon code that is used to encode the data stream in digital communication. The performances were evaluated by applying to binary phase shift keying modulation scheme in symmetric Additive White Gaussian Noise channel. Reed-Solomon codes are best for correcting burst errors and find wide range of applications in digital communications and data storage.

Keywords

Reed-Solomon codes (RS), Forward Error Correction (FEC), Additive White Gaussian Noise (AWGN), Binary Phase Shift Keying (BPSK).

1. OVERVIEW ON CODING

Channel coding for error detection and correction helps the communication system designers to reduce the effects of a noisy transmission channel. Error control coding theory has been the subject of intense study since the 1940s and now being widely used in communication systems. As illustrated by Shannon in his paper published in 1948 [1], for each physical channel there is a parametric quantity called the channel capacity C that is a function of the channel input output characteristics. Shannon showed that there exist error control codes such that arbitrary small error probability of the data to be transmitted over the channel can be achieved as long as the data transmission rate is less than the capacity of the channel.

During digital data transmission and storage operations, performance criterion is commonly determined by BER which is simply: Number of error bits / Number of total bits. Noise in transmission medium disturbs the signal and causes data corruptions. Relation between signal and noise is described with SNR (signal-to-noise ratio). Generally, SNR is explained with signal power / noise power and is inversely proportional with BER. It means, the less the BER result is the higher the SNR and the better communication quality [2].

Mainly there are two types of Forward Error Correction (FEC) coding techniques: linear block coding and convolution encoding [3]. Reed-Solomon codes come under the category of linear block codes.

A generic block diagram of digital communication system is shown in Fig.1 [5]. The binary digits from the encoder are fed into a modulator, which maps them into one of the known digital modulation waveforms, say BPSK or BFSK. The channel over which the waveforms are transmitted will corrupt the waveforms in general by adding symmetric additive white Gaussian noise (AWGN). The resulting received noisy signal is demodulated to its binary regime and decoded back to the original binary information sequence. The decoding decision scheme may be one of two possible decoding schemes hard or soft decision scheme. In the hard decision decoding, the demodulator quantized the incoming signal into two levels, denoted as 0 and 1. The information sequence bits are then recovered by the decoder that will have a certain error correcting capability. On the other hand, if the unquantized (analog) demodulator output is fed to the decoder we call this decoding scheme soft decision decoding. This paper shows the basic concept of RS codes and various simulations that are performed to find out the best BER performance of the RS codes for different code rates. All the simulations are performed using MATLAB Software.

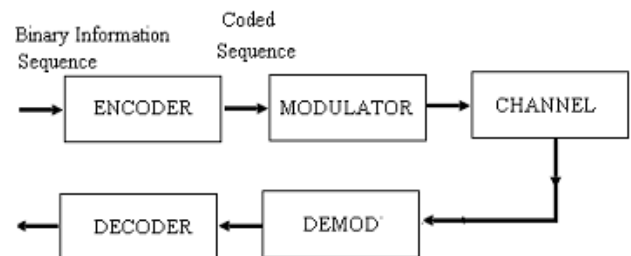


Fig 1: Block diagram of digital communication system with channel coding

2. LINEAR BLOCK CODES

For a block of k message bits, $(n-k)$ parity bits or check bits are added. This means that the total bits at the output of channel encoder are n . Such types of codes are known as (n,k) block codes. In the systematic block code, message bits appear at the beginning of the code word. As shown in the figure2 the message bits appear first and then check bits are transmitted in a block. This type of code is known as the systematic code[4].

A block code c is constructed by breaking up the message data stream into blocks of length k and has the form $(m_0, m_1, \dots, m_{k-1})$, and mapping these blocks into code words in c . The resulting code consists of a set of M code words $(c_0, c_1, \dots, c_{M-1})$. Each code word has a fixed length denoted by n and has a form $(c_0, c_1, \dots, c_{n-1})$. The elements of the code word are selected from an

alphabet field of q elements. In the binary code case, the field consists of two elements, 0 and 1. On the other hand, when the elements of the code word are selected from a field that has q alphabet elements, the code is non binary code. As a special case when q is a power of 2 (i.e. $q = 2^m$) where m is a positive integer, each element in the field can be represented as a set of distinct m bits.

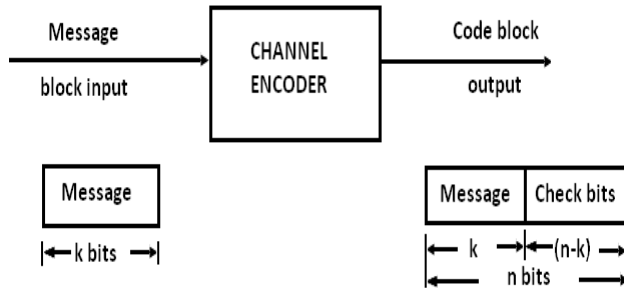


Fig 2: Functional block diagram of a block coder

As indicated above, codes are constructed from fields with a finite number of q elements called Galois field and denoted by $GF(q)$. In general, finite field $GF(q)$ can be constructed if q is a prime or a power of prime number. When q is a prime, the $GF(q)$ consist of the elements $\{0, 1, 2, \dots, q-1\}$ with addition and multiplication operations are defined as a modulo- q . If q is a power of prime (i.e. $q = p^m$ where m is any positive integer), it is possible to extend the field $GF(p)$ to the field $GF(q = p^m)$. This is called the extension field of $GF(p)$ and in this case multiplication and addition operations are based on modulo- p arithmetic.

3. INTRODUCTION TO RS CODES

Reed-Solomon codes are block-based error correcting codes with a wide range of applications in digital communications and storage. It is vulnerable to the random errors but strong to burst errors. Hence, it has good performance in fading channel which have more burst errors. In coding theory Reed-Solomon (RS) codes are cyclic error correcting codes invented by Irving S. Reed and Gustave Solomon. They described a systematic way of building codes that could detect and correct multiple random symbol errors. By adding t check symbols to the data, an RS code can detect any combination of up to t erroneous symbols, and correct up to $\lfloor t/2 \rfloor$ symbols. As an erasure code, it can correct up to t known erasures, or it can detect and correct combinations of errors and erasures. Reed-Solomon codes are used to correct errors in many systems including:

- Storage devices (including tape, Compact Disk, DVD, barcodes, etc)
- Wireless or mobile communications (including cellular telephones, microwave links, etc)
- Satellite communications
- Digital television / DVB
- High-speed modems such as ADSL, xDSL, etc.

The Reed-Solomon encoder takes a block of digital data and adds extra "redundant" bits. Errors occur during transmission or storage for a number of reasons (for example noise or interference, scratches on a CD, etc). The Reed-Solomon decoder processes each block and attempts to correct errors and recover the original data. The number and type of errors that can

be corrected depends on the characteristics of the Reed-Solomon code.

3.1 Historical Background

On January 2, 1959, Irving Reed and Gus Solomon submitted a paper to the Journal of the Society for Industrial and Applied Mathematics. In June of 1960 the paper was published: five pages under the rather unpretentious title "Polynomial Codes over Certain Finite Fields". This paper described a new class of error-correcting codes that are now called Reed-Solomon codes. In the decades since their discovery, Reed-Solomon codes have enjoyed countless applications, from compact disc™ players in living rooms all over the planet to spacecraft that are now well beyond the orbit of Pluto. Reed-Solomon codes have been an integral part of the telecommunications revolution in the last half of the twentieth century [10].

4. ENCODING OF RS CODES

Reed Solomon codes are a subset of BCH codes and are linear block codes. A Reed-Solomon code is specified as RS (n, k) with s -bit symbols. This means that the encoder takes k data symbols of s bits each and adds parity symbols to make an n symbol codeword. There are $n-k$ parity symbols of s bits each. A Reed-Solomon decoder can correct up to t symbols that contain errors in a codeword, where $2t = n-k$.

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. The amount of processing "power" required to encode and decode Reed-Solomon codes is related to the number of parity symbols per codeword. A large value of t means that a large number of errors can be corrected but requires more computational power than a small value of t [6].

5. DECODING OF RS CODES

Reed-Solomon algebraic decoding procedures can correct errors and erasures. An erasure occurs when the position of an erred symbol is known. A decoder can correct up to t errors or up to $2t$ erasures. Erasure information can often be supplied by the demodulator in a digital communication system, i.e. the demodulator "flags" received symbols that are likely to contain errors [7].

When a codeword is decoded, there are three possible outcomes:

1. If $2s + r < 2t$ (s errors, r erasures) then the original transmitted code word will always be recovered,

OTHERWISE

2. The decoder will detect that it cannot recover the original code word and indicate this fact.

OR

3. The decoder will mis-decode and recover an incorrect code word without any indication.

The probability of each of the three possibilities depends on the particular Reed-Solomon code and on the number and distribution of errors.

5.1 Coding Gain

The advantage of using Reed-Solomon codes is that the probability of an error remaining in the decoded data is (usually)

much lower than the probability of an error if Reed-Solomon is not used. This is often described as coding gain.

6. ARCHITECTURES FOR ENCODING AND DECODING RS CODES

Reed-Solomon encoding and decoding can be carried out in software or in special-purpose hardware.

6.1 Finite (Galois) Field Arithmetic

Reed-Solomon codes are based on a specialist area of mathematics known as Galois fields or finite fields. A finite field has the property that arithmetic operations (+, -, x, / etc.) on field elements always have a result in the field. A Reed-Solomon encoder or decoder needs to carry out these arithmetic operations. These operations require special hardware or software functions to implement [8,9].

6.2 Generator Polynomial

A Reed-Solomon codeword is generated using a special polynomial. All valid codewords are exactly divisible by the generator polynomial. The general form of the generator polynomial is:

$$g(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{2t})$$

and the codeword is constructed using:

$$c(x) = g(x) \cdot i(x)$$

where $g(x)$ is the generator polynomial, $i(x)$ is the information block, $c(x)$ is a valid codeword and a is referred to as a primitive element of the field. Example: Generator for RS(255,249)

$$g(x) = (x - \alpha_0)(x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)(x - \alpha_5)$$

$$g(x) = x_6 + g_5x_5 + g_4x_4 + g_3x_3 + g_2x_2 + g_1x_1 + g_0$$

6.3 Encoder architecture

The $2t$ parity symbols in a systematic Reed-Solomon codeword are given by:

$$p(x) = i(x) \cdot x^{n-k} \bmod g(x)$$

An architecture for a systematic RS (255,249) encoder each of the 6 registers holds a symbol (8 bits). The arithmetic operators carry out finite field addition or multiplication on a complete symbol.

6.4 Decoder architecture

The received codeword $r(x)$ is the original (transmitted) codeword $c(x)$ plus errors:

$$r(x) = c(x) + e(x)$$

A Reed-Solomon decoder attempts to identify the position and magnitude of up to t errors (or $2t$ erasures) and to correct the errors or erasures. Decoding is done by adopting the following steps:

Syndrome Calculation

This is a similar calculation to parity calculation. A Reed-Solomon codeword has $2t$ syndromes that depend only on errors (not on the transmitted code word). The syndromes can be calculated by substituting the $2t$ roots of the generator polynomial $g(x)$ into $r(x)$.

Finding the Symbol Error Locations

This involves solving simultaneous equations with t unknowns. Several fast algorithms are available to do this. These algorithms take advantage of the special matrix structure of Reed-Solomon codes and greatly reduce the computational effort required.

Find an error locator polynomial

This can be done using the Berlekamp-Massey algorithm or Euclid's algorithm. Euclid's algorithm tends to be more widely used in practice because it is easier to implement: however, the Berlekamp-Massey algorithm tends to lead to more efficient hardware and software implementations.

Find the roots of this polynomial

This is done using the Chien search algorithm.

Finding the Symbol Error Values

Again, this involves solving simultaneous equations with t unknowns. A widely-used fast algorithm is the Forney algorithm.

7. APPLICATIONS OF RS CODES

a) The Digital Audio Disc

It can safely be claimed that Reed-Solomon codes are the most frequently used digital error control codes in the world. This claim rests firmly on the fact that the digital audio disc, or compact disc uses Reed-Solomon codes for error correction and error concealment. Special properties of Reed-Solomon codes make the sound quality of the compact disc as impressive as it is (the signal-to-noise ratio at the output exceeds 90 dB). The compact disc system uses a pair of cross-interleaved Reed-Solomon codes.

b) Deep Space Telecommunication Systems

McEliece and Swanson examined the use of Reed-Solomon codes in several of NASA and ESA's planetary exploration missions. However, when convolutional and Reed-Solomon codes are used in concatenated systems, enormous coding gains are achievable. A convolutional code is used as an "inner code," while a Reed-Solomon code is used to correct errors at the output of the convolutional (Viterbi) decoder. The Viterbi decoder output happens to be bursty, providing a perfect match for a Reed-Solomon code. The most famous application of the concatenated convolutional/Reed-Solomon system was in the Voyager expeditions to Uranus and to Neptune [11].

c) Error Control for Systems with Feedback

Wicker and Bartz examine various means for using Reed-Solomon codes in applications that allow the transmission of information from the receiver back to the transmitter. Such applications include mobile data transmission systems and high-reliability military communication systems. Along with their powerful error correction capabilities, Reed-Solomon codes can also provide a substantial amount of simultaneous error detection.

d) Spread-Spectrum Systems

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

e) Satellite Broadcasting (DVB)

The demand for satellite transponder bandwidth continues to grow, fueled by the desire to deliver television (including new channels and High Definition TV) and IP data. Transponder availability and bandwidth constraints have limited this growth, because transponder capacity is determined by the

selected modulation scheme and Forward Error Correction (FEC) rate. BPSK coupled with traditional Reed Solomon and Viterbi codes have been used for nearly 20 years for the delivery of digital satellite TV.

8. SIMULATION RESULTS

A full system model was implemented in Matlab. Performance analysis of RS codes is done for different code rates by taking random data stream. Here we have used BPSK (Binary Phase Shift Keying) modulation and demodulation for all the simulations. The encoded data is then passed through Gaussian channel which adds Additive White Gaussian Noise (AWGN) to the channel symbols produced by the encoder. In the following figures, E_b/N_0 dB denotes the information bit energy to noise power density ratio and at the y-axis we plot the bit error rate (BER).

First we run the simulations for RS codes with different code rates i.e. 0.96, .878, .80 and .647. These simulations are carried out for constant block length or codeword length which is 255. From figure3, it can be seen, as we decrease the code rate keeping block length constant the BER performance improves. We can see that the absolute BER performance is approx. 2dB better for 0.647 code rate than 0.96 at BER of 0.0066.

Next we performed the simulations for RS codes for different code rates as well as block lengths. We can see from the figure 4, as the block length increases the BER performance also improves. So here the best result comes out with RS (400,240) with $m=9$ i.e. number of bits per symbol is 9.

We can now say that for RS codes the BER performance improves with the decreasing code rate and to some how large block lengths. The RS code, which is well suited for correction of burst errors, shows a poor BER performance for lower SNR values, because of the mainly random errors introduced by the AWGN

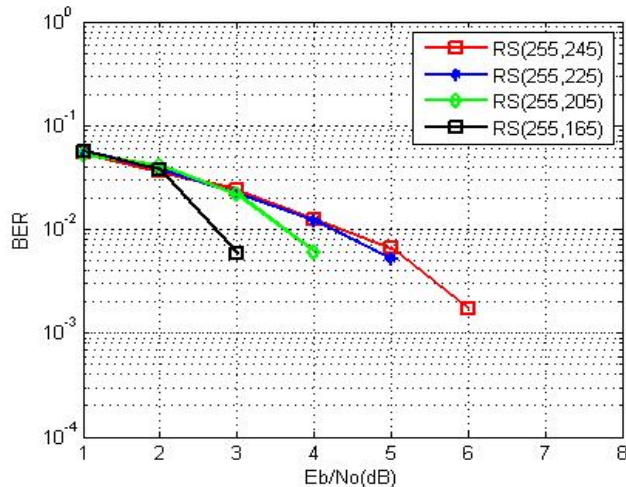


Fig 3: The BER performance comparison of RS codes for different code rates and fixed block length of 255

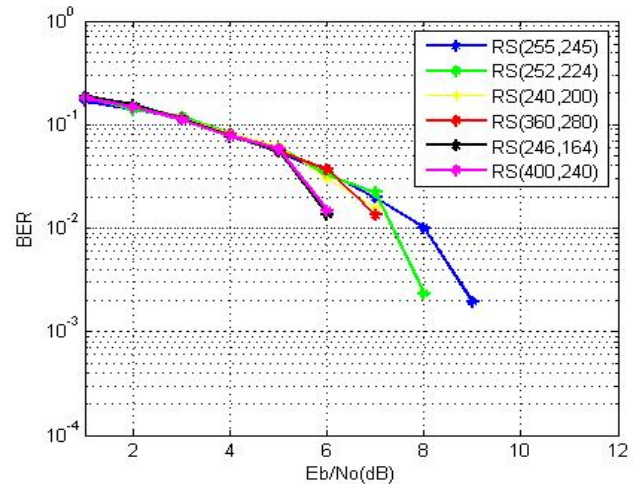


Fig 4: The BER performance comparison of RS codes for different code rates and block lengths

9. CONCLUSION

Through this paper we present the deep and clear understanding of Reed-Solomon codes making them simpler and easier to understand and implement. RS codes are finding increasing use in applications where reliable and highly efficient information transfer over bandwidth in the presence of data-corrupting noise is desired like recently, RS codes have been considered for many industrial standards of next generation communication systems. The purpose of this paper is to study the Reed-Solomon (RS) code, with an aim to simulate the encoding and decoding processes. In this paper we performed the simulations of Reed-Solomon codes for different code rates keeping block length constant. It was concluded that the BER performance improves as the code rate decreases. The simulations also showed that the BER performance also improves for large block lengths and RS codes shows a poor BER performance for lower SNR. As the SNR value increases the curve becomes steeper.

10. REFERENCES

- [1] C. E. Shannon: "A mathematical theory of communication," Bell System Technical Journal, vol. 27, October 1948, pp. 379–423.
- [2] C. Berrou, A. Glavieux and P. Thitimajshima, "Near Shannon Limit Error-Correcting Coding and Decoding: Turbo codes", ICC' 93, Conference Record, Geneva, pp. 1064–1070, 1993.
- [3] Daniel J., Costello, JR., Error Control Coding, Fundamentals and Applications, Prentice Hall, Inc. Englewood Cliffs, New Jersey, 1983
- [4] S. Lin and D.J. Costello, Jr. Error Control Coding: Fundamentals and Applications, Englewood Cliffs, NJ: Prentice Hall, 1983
- [5] J. Proakis, Digital communications, NY: McGraw Hill, 2001
- [6] I.S. Reed and G. Solomon, "Polynomial Codes Over Certain Finite Fields," SIAM Journal of Applied Mathematics, vol. 8, 1960, pp. 300–304.

- [7] R.J.McEliece, L.Swanson, "On the decoder error probability for Reed-Solomon codes", IEEE Trans.on Inf.Theory, Vol.IT-32, pp.701-703
- [8] [3] R. E. Blahut, "Transform Techniques for Error Control Codes," IBM Journal of Research and Development, Volume 23, pp. 299-315, 1979.
- [9] S. B. Wicker, Error Control Systems for Digital Communication and Storage, Englewood Cliffs, N.J.: Prentice-Hall, 1994.
- [10] I. S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Fields," SI AM Journal of Applied Mathematics, Volume 8, pp. 300-304,1960.
- [11] J.L. Massey, "Deep Space Communications and Coding: A Match Made in Heaven," in Advanced Methods for Satellite and Deep Space Communications, J. Hagenauer (ed.), Lecture Notes in Control and Information Sciences, Volume 182, Berlin: Springer-Verlag, 1992.