International Journal of Engineering Research-Online
A Peer Reviewed International Journal
Articles available online http://www.ijoer.in

Vol.3., Issue.5., 2015
(Sept.-Oct.)

RESEARCH ARTICLE

ISSN: 2321-7758

VHDL IMPLEMENTATION OF REED-SOLOMON CODE FOR EFFICIENT COMMUNICATION SYSTEM

PANKAJ KUMAR JHA[1], MONIKA KAPOOR[2]
[1]Scholar, M.Tech, LNCT Bhopal
[2]Associate Professor, LNCT Bhopal

PANKAJ KUMAR JHA

ABSTRACT

In the communication systems, RS codes have a widespread use to provide error protection. For burst errors and random errors, RS code has become a popular choice to provide data integrity due to its good error correction capability. This feature has been one of the important factors in adopting RS codes in many practical applications such as wireless communication system, cable modem, computer memory and ADSL systems. Reed Solomon codes are an important sub class of non-binary BCH codes. These are cyclic codes and are very effectively used for the detection and correction of burst errors. Galois field arithmetic is used for encoding and decoding of reed Solomon codes. The design experience will be formulated to form the complete design methodology of the FEC modules at the register-transfer level (RTL). Then we incorporate the knowledge into our RS code generator design flow.

Keywords—ADSL, BCH Codes, Galois field, Random errors, Reed Solomon,

INTRODUCTION

Digital communication system is used to transport information bearing signal from the source to a user destination via a communication channel. The information signal is processed in a digital communication system to form discrete messages which makes the information more reliable for transmission. Channel coding is an important signal processing operation for the efficient transmission of digital information over the channel. It was introduced by Claude E. Shannon in 1948 by using the channel capacity as an important parameter for error free transmission. In channel coding the number of symbols in the source encoded message is increased in a controlled manner in order to facilitate two basic objectives at the receiver one is Error detection and other is Error correction. Error detection and Error correction to achieve good communication is also employed in devices. It is used to reduce the level of noise and interferences in electronic medium. Channel coding for error detection and correction helps the communication system designers to reduce the effects of a noisy transmission channel.

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

The aim of the project is to correct multiple random errors and burst errors that are occur during the transmission of the information by using Reed Solomon codes. The proposed code is designed using verilog coding and the results demonstrate that the reed Solomon codes are very efficient for the detection and correction of burst errors.

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 performance of the RS codes for different code rates.

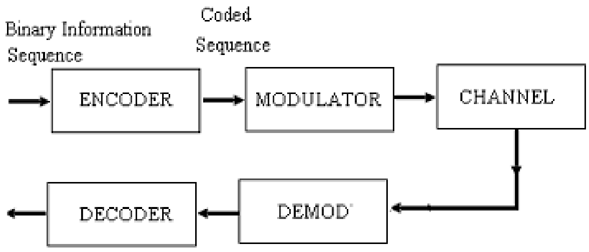

Fig 1: Block diagram of digital communication system with channel coding

Linear Block Code

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.

A block code c is constructed by breaking up the message data stream into blocks of length k and has the form (mo, m1,…..mk-1), and mapping these blocks into code words in c. The resulting code consists of a set of M code words (co, c1,……..cM-1). Each code word has a fixed length denoted by n and has a form (co, c1,……..cn-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 = 2m) where m is a positive integer, each element in the field can be represented as a set of distinct m bits.

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,….q -1}with addition and multiplication operations are defined as a modulo-q . If q is a power of prime (i.e. q = pm where m is any positive integer), it is possible to extend the field GF (p) to the field GF (q = pm). This is called the extension field of GF (p) and in this case multiplication and addition operations are based on modulo- p arithmetic.

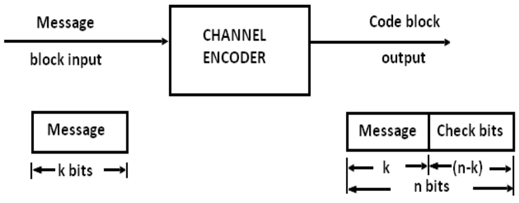

Fig 2: Functional block diagram of a block coder

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

Reed Solomon Code

The Reed Solomon code is an algebraic code belonging to the class of BCH (Bose-Chaudhry-Hocquehen) multiple burst correcting cyclic codes. The Reed Solomon code operates on bytes of fixed length. Given m parity bytes, a Reed Solomon code can correct up to m byte errors in known positions (erasures), or detect and correct up to m/2 byte errors in unknown positions. This is an implementation of a Reed Solomon code with 8 bit bytes, and a configurable number of parity bytes. The maximum sequence length (code word) that can be generated is 255 bytes, including parity bytes. In practice, shorter sequences are used.

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. 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. 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.

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.

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.

Architecture of RS Codes

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

A. 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

B. 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-αi)(x-αi+1)….(x-αi+2t)

and the codeword is constructed using:

c(x) = g(x).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-α0) (x-α1) (x-α2) (x-α3) (x-α4) (x-α5)

g(x) = x6 + g5x5 + g4x4 + g3x3 + g2x2 + g1x1 + g0

C. *Encoder Architecture*

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

p(x) = i(x). xn-k mod 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.

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

Simulation Results

A full system model was implemented in VHDL. The following results are obtained.

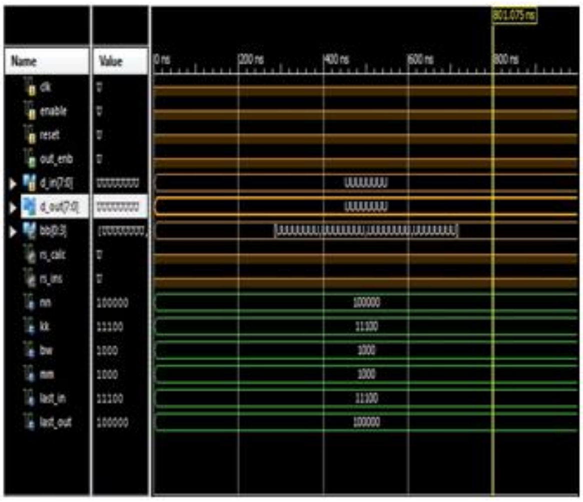

Fig 3: Simulation result for Encoder

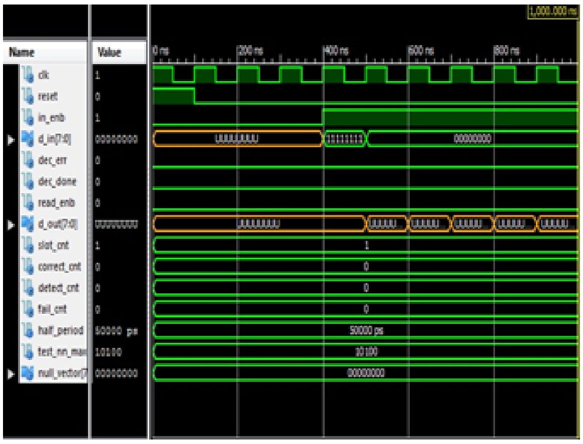

Fig 4: Simulation result for Decoder

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.

References

[1]. Daniel J., Costello, JR., Error Control Coding, Fundamentals and Applications, Prentice Hall, Inc. Englewood Cliffs, New Jersey, 1983

[2]. 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

[3]. R. E. Blahut, "Transform Techniques for Error Control Codes," IBM Journal of Research and Development, Volume 23, pp. 299-315, 1979.

[4]. S. B. Wicker, Error Control Systems for Digital Communication and Storage, Englewood Cliffs, N.J.: Prentice-Hall, 1994

[5]. I. S. Reed and G. Solomon, "Polynomial Codes over Certain Finite Fields," SI AM Journal of Applied Mathematics, Volume 8, pp. 300-304,1960.

[6]. 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.