International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Design and Implementation of Reed Solomon (16, 8) Decoder

Sheetal Sudhakaran† **and Ramesh P.†**

†Department of Electronics and Communication, CUSAT, College of Engineering Munnar, Kerala, India

Accepted 02 June 2015, Available online 10 June 2015, **Vol.5, No.3 (June 2015)**

Abstract

Channel coding can use either Automatic Repeat request or Forward Error Correction technique depending on the properties of the system or on the application in which the error correcting is to be introduced. It is an important operation for the digital communication system transmitting digital information over a noisy channel. Error control coding techniques are based on the addition of redundancy to the information message according to a prescribed rule thereby providing data a higher bit rate. The combined goal of the channel encoder and the decoder is to minimize the channel noise. RS codes are non-binary cyclic error correcting block codes. Here redundant symbols are generated in the encoder using a generator polynomial and added to the very end of the message symbols. Then RS Decoder determines the locations and magnitudes of errors in the received polynomial. Galois field arithmetic is used for encoding and decoding of Reed – Solomon codes. Verilog implementation creates a flexible, fast method and high degree of parallelism for implementing the Reed – Solomon codes. The design is carried out by writing Verilog modules for different encoder and decoder components. The results constitute simulation of Verilog codes of different modules of the Reed – Solomon Codes.

Keywords: *Code word, Galois field, RS encoder, RS decoder, Verilog.*

1. Introduction

Digital communication system is used to transport an 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. 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: error detection and error correction. Error detection and error correction to achieve good communication is also employed in electronic devices. It is used to reduce the level of noise and interferences in electronic medium. Error correcting codes have a wide range of applications in different fields like digital data communications, memory system design etc. Reed Solomon (RS) codes, encoders and decoders are extremely powerful error correcting tools that increase transmission quality to a great extent.

2. Concurrent Error Correction Schemes

Error-correcting codes (ECC) were first developed in the 1940s following a theorem of Claude Shannon that showed that almost error-free communication could be obtained over a noisy channel. The quality of the recovered signal will however depend on the error correcting capability of the codes. Generally linear cyclic codes are used for channel coding. The work of Shannon demonstrated that even though communication channels are subject to noise and errors, if some amount of redundancy is encoded into the signal, errors can be accounted for and corrected at the receiving end. This is the fundamental principle of error-correction coding schemes, and has led to the development of various encoding schemes. In 1948, Shannon introduced the linear block codes for complete correction of errors. Cyclic codes were first discussed by Prange. This led directly to the work published in1960 by Bose and Roy-Chaudhuri the BCH codes. In 1959, Irving Reed and Solomon described a new class of error-correcting codes called Reed-Solomon codes. RS codes have been one of the most widely used ECC schemes, mainly because the coding scheme allows for efficient correction of both burst and random errors. RS is a block scheme because it encodes blocks of a specific amount of data individually, as opposed to operating on the entire data stream as a whole.

Error correction coding requires lower rate codes than error detection, but is a basic necessity in safety critical systems, where it is absolutely critical to get it right first time itself. In these special circumstances,

*Corresponding author: **Sheetal Sudhakaran** is a M.Tech Scholar and **Ramesh P.** is working as Associate Professor

the additional bandwidth required for the redundant check-bits is an acceptable price.

3. Reed Solomon encoding and decoding

The most notable error correcting codes are Reed Solomon codes. In real world communication, errors are introduced in messages sent from one point to another. Reed Solomon is an error-correcting coding system that was devised to address the issue of correcting multiple errors - especially burst-type errors. 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.

3.1 Galois field

The theory of error control codes uses a mathematical construct known as finite fields or Galois fields (GFs). A GF is a set that contains a finite number of elements. The operations of addition and multiplication on this set are defined and the operations behave as would be expected from normal arithmetic. A Finite Field is a field with a finite field order (i.e., number of elements), also called a Galois field .For example ,the additive identity element is 0 and the multiplicative identity element is 1. RS codes operate on GFs of order q = pm where p is a prime positive integer and m is a positive integer. A GF of order q is denoted by GF(q) and it contains q distinct elements. The elements of a GF are typically denoted using the variable. The elements of GF(8) have different notations. Elements are typically represented using either power or polynomial notation when performing calculations by hand, but binary notation is used when the codes are actually implemented in hardware. All three notations are simply three different ways to represent a given GF element. Multiplication is easier in power notation because the exponents are added. Similarly, addition is easier in polynomial notation. Numerous books and computer programs exist that list or generate the elements for GFs of various sizes.

3.2 Reed Solomon codes

Reed Solomon (RS) codes , encoders and decoders are extremely powerful error correcting tools that increase transmission quality to a great extent. They are well understood, relatively easy to implement provides a good tolerance to error bursts and is compatible with binary transmission systems. RS codes operate on the information by dividing the message stream into blocks of data, adding redundancy per block depending only on the current inputs. The symbols in RS coding are elements of a finite field or Galois Field (GF).

For RS (16,8) code, n = block length = 16, k = no. of un-coded massage symbols= 8, 2t = (n-k) = number of parity symbols =8, t = maximum number of errors can be corrected =4. The original massage can be recovered by employing the RS decoder provided number of errors in the received codeword is less than or equal to four.

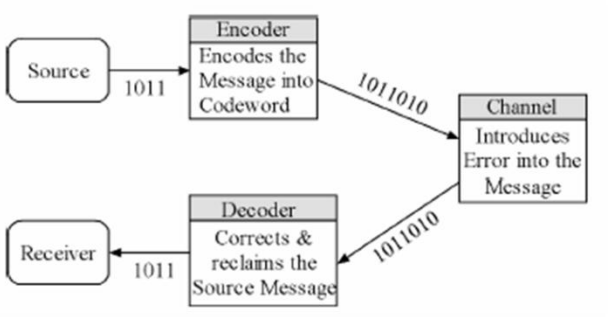

Fig. 1 Reed Solomon Protected Channel

Encoding is achieved by affixing the remainder of a GF polynomial division into the message. This division is accomplished by a Linear Feedback Shift Register (LFSR) implementation. The mathematics of RS encoding is based on finite field arithmetic .GF multipliers are used for encoding the information block. The function of the decoder is to process the received codeword to compute an estimate of the original message symbols.

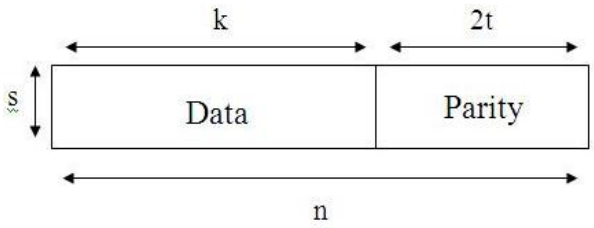

Fig.2 Structure of RS codeword

Typically about ten times more resources are required to decode and correct the corrupted data. The codes are represented by the format RS (n, k) where n is the total number of s-bit wide symbols, and k is the number of s-bit wide information (data)symbols in a codeword. RS Decoder performs detection and correction of information (data) symbols in a codeword. The RS encoder provided at the transmitter end encodes.

The input message into a codeword and transmits the same through the channel. Noise and other disturbances in the channel may disrupt and corrupt the codeword. This corrupted codeword arrives at the receiver end (decoder). Once the number of errors is determined, the decoder decides if they are within the range of correction. After determining this, the decoder corrects the errors in the received data. In the next two sections a detailed insight into the encoding and decoding processes of these RS codes are provided.

3.3 RS encoder

Encoding is a process of converting a input message into a corresponding codeword. The key to the RS encoding is to view the symbols of the message that is to be encoded as if they are the coefficients of a polynomial. 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 generator polynomial. The general idea is the construction of a polynomial, the coefficient produced will be symbols such that the generator polynomial will exactly divide the data or parity polynomial. The transmitted codeword is systematically encoded.

Operation

RS codes are systematic, so for encoding, the information symbols in the codeword are placed as the higher power coefficients. Any RS encoder design should effectively perform the following two operations, namely division and shifting. Both operations can be easily implemented using Linear-Feedback Shift Registers.

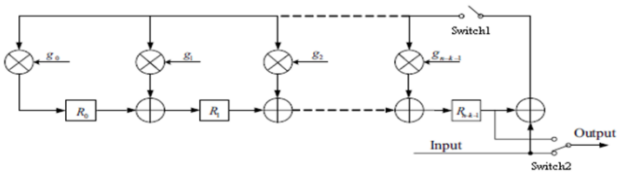

Fig. 3 Encoder Architecture

The encoder block diagram shows that one input to each multiplier is a constant field element, which is a coefficient of the polynomial g(x). For a particular block, the information polynomial M(x) is given into the encoder symbol by symbol. These symbols appear at the output of the encoder after a desired latency, where control logic feeds it back through an adder to produce the related parity. This process continues until all of the k symbols of M(x) are input to the encoder. During this time, the control logic at the output enables only the input data path, while keeping the parity path disabled.

During the first k clock cycles, the feedback control logic feeds the adder output to the bus. After the last symbol has been input into the encoder a wait period of at least n-k clock cycles occurs. During this waiting time, the feedback control logic disables the adder output from being fed back and supplies a constant zero symbol to the bus. Also, the output control logic disables the input data path and allows the encoder to output the parity symbols.

3.4 RS decoder

The Reed Solomon decoder tries to correct errors 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. These errors are corrected using the chien search algorithm. For an RS (n, k) code where n - k = 2T, the decoder can correct up to T symbol errors in the code word.

Operation

When a RS Decoder corrects a symbol, it replaces the incorrect symbol with the correct one, whether the error was caused by one bit being corrupted or all of the bits being corrupted. This gives RS codes tremendous burst-noise advantages over binary codes . RS Decoder mainly works on five steps:

1. Calculate the syndromes.
2. Use the syndromes to determine the "error locator polynomial."
3. Find the roots of the error locator polynomial. The inverses of these roots give the locations of errors.
4. Use the syndromes, roots, and error locator polynomial to determine the error magnitudes.
5. Use the information about error location and magnitude to actually correct the errors.

The first step is to calculate the syndrome values from the received codeword R(x). Here the input received symbols are divided by the generator polynomial. The result should be zero. The parity is placed in the codeword to ensure that code is exactly divisible by the generator polynomial. If there is a remainder, then there are errors. The remainder is called the syndrome. The syndromes can then be calculated by substituting the 2t roots of the generator polynomial g(x) into R(x). The next step, after the computing the syndrome polynomial is to calculate the error values and their respective locations. Syndrome values are used to find the coefficients of the error locator polynomial and the error magnitude polynomial .The berlekamp algorithm is used to find error locations . Once the error locator(x) and error evaluator (x) polynomials have been determined, the next step in the decoding process is to evaluate the error polynomial. Chien search algorithm is used for that.

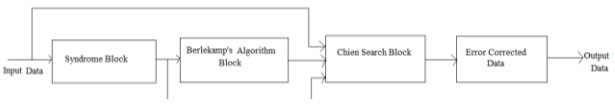

Fig.4 RS Decoder Block diagram

4. Simulation Results

The goal of this work is to implement a Reed Solomon encoder and decoder. The RS encoder design should effectively perform division and shifting. Both operations can be easily implemented using Linear-

Feedback Shift Registers. The simulation result of RS decoder is shown below.

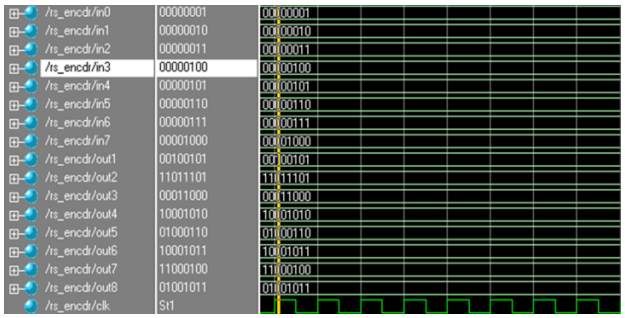

Fig.5 Encoder output

The RS decoder (16, 8) mainly consist of 3 blocks Syndrome Block, Berlekamp's algorithm block and Chien Search block. If there is no error in the data Syndrome values are zero.

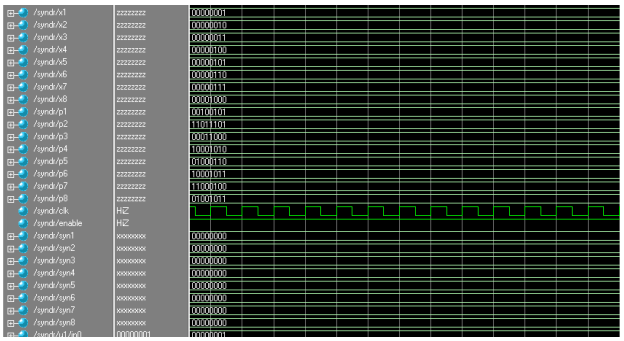

Fig.6 Syndrome Block output

Berlekamp's Algorithm Evaluate the error locations.
If the determinant value D is zero .Then it means there are no error locations.

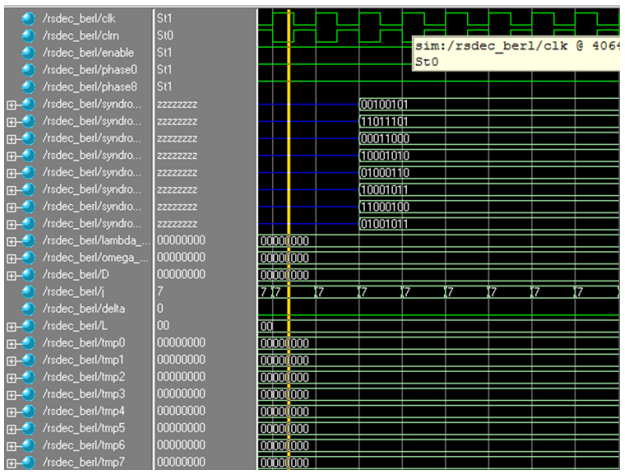

Fig.7 Berlekamp's Algorithm block

If any error exists, chien search block corrects the error. If there is no error, value of omega and lambda are zero.

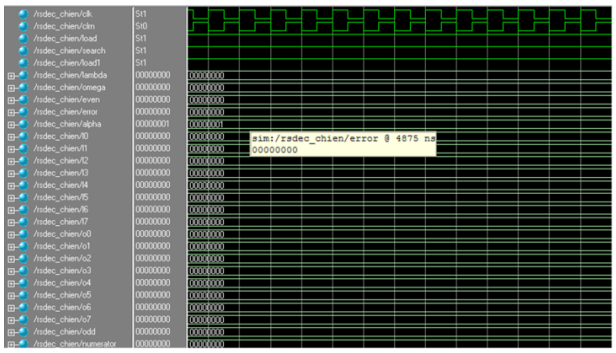

Fig.8 Chien Search Block

In the chien search block output, the data is received.

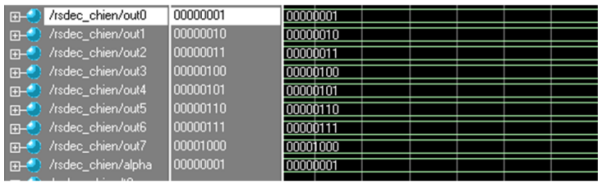

Fig.9 Output Data

Conclusions

In this work design and implementation of RS Encoder and Decoder (16, 8) was presented. The results constitute simulation of verilog codes of different modules of the Reed Solomon codes .Here error detection and correction techniques have been used which are essential for reliable communication over a noisy channel. The result demonstrates that the Reed Solomon codes are useful for the detection and correction of burst errors. As the future work RS decoder for the error correction in compact disk can be developed. RS codes are used significantly in Wireless Communication (mobile phones), Deep Space and Satellite Communications Networks mass storage devices (compact disk, DVD), digital TV, digital video broadcasting (DVB).

References

E. Berlekamp, R. Peile, and S. Pope.(1987), IEEE Communications Magazine, *The application of error control to communications*, vol. 25, no. 4, pp. 44–57.

S. Bernard.(2001), Prentice Hall ,*Digital communications fundamentals and applications.*

R. C. Bose and D. K. Ray-Chaudhuri.(1960), Information and Control, *Further results on error correcting binary group codes,* vol. 3, no. 3, pp. 279–290.

T. Oberg(2001), John Wiley & Sons, *Modulation, detection and coding.*

G. Orlando and C. Paar.(1999), Field-Programmable Custom Computing Machines, *A super-serial Galois fields multiplier for FPGAs and its application to public-key algorithms* ,pp. 232–239.

E. Prange.(1957), Air Force Cambridge Research Center, *Cyclic Error-Correcting codes in two symbols.*

M. Purser and A. House.(1995), Artech House Boston *Introduction to error-correcting codes.*

I. S. Reed and G. Solomon (1960), Journal of the Society for Industrial & Applied Mathematics, *Polynomial codes over certain finite fields,* vol. 8, no. 2, pp. 300–304,