Design ofRS Code Using Simulink Platform

B. K. Mishra Sukruti Kaulgud Sandhya Save
Thakur College of Engineering and Technology
Kandivli(East), Mumbai-101

ABSTRACT

Reed–Solomon (RS) codes are non-binary cyclic error correcting codes widely used for robust and energy efficient transmissions. They are block-based error correcting codes with a wide range of applications in digital communications like digital audio and vidco, magnetic and optical recording,computcr memory, cable modem. xDSLwireless andsatellite connnunications systems etc.

In this work, we proposed Simulink based modelfor performance analysis of the RS (n,k) code architecture and implement the same on FPGA.The experimental results of RS encoder simulationconfirm that this model isfast and parameterizable. The biggest advantage of this method, it can be implemented on FPGAwith less amount of logic blocks saving area and time. This feature makes it an attractive method for SoC application**.**

Index Terms—Reed Solomon codes, FPGA, Matlab Simulink, SoC, error correcting codes .

1.INTRODUCTION

The rapidly growing demand for ubiquitous communicationand computing has resulted in an exponential growth in theamount of data generated and stored. Also, this has dramaticallychanged the way we store, manage, search and accessinformation. Digital audiodisks and compact disks use RS codes for error correctionand concealment.

Traditionally Reed Solomon (RS) codes have beenlargely employed as channel codes due to their excellenterror detection and correction properties. Theirremarkable capability of recovering combinations ofrandom **as** well as burst errors makes RS codes theideal choice in a lot of applications.RS codeswere also successfully exploited, during **NASA** andESA planetary exploration missions, in deep spacetransmissions.This **RS** code and theimplementation **are** universal in the sense that the sameVLSI chips ***can*** be applied for variety of codes withdifferent code length, different dimension and differentminimum distance, **as** well **as** for different transmissiondata rate and different packet length.

For reliable space communication thereis a need to use RS codes with large error-correcting capability andlarge interleaving level. Hence, one is especially interestedin minimizing the complexity of RSencoders for spacecommunication applications. In a spacecraft the power, size, andreliabilityrequirements are usually quite severe. Thus, there is considerableinterest in a VLSI (very large scaleintegration) RS encoderwhich has the potential for significant savings in size, weight, andpower, while at the same time providing higher reliability over an RSencoder implemented in discrete logic circuits.

Due to so many applications of REED Solomon codes this paper concentrates on design of RS codes. This paper makes this design platform independent by designing RS codes using simulink.

1.CODE COMPARISON

The general strategy for pin-pointing errors is to send messages with repetition. This repetition allows for some of the data to be corrupted while still retaining the ability to decode the original message. Using this repetition optimally is the challenge for modern day error codes. There is a provable maximum accuracy (called the Shannon limit), but while it is theoretically interesting to know that there is fundamentally a 'best' code, it does not create a practical code that functions at this limit. This section will look into the different error correcting codes that have practical value and deal with the advantages and disadvantages associated with these codes rather than their specifics.

Hamming Codes send m information bits padded with a specific k parity-check bits[3]. They have the ability to correct any single mistake. They manage this by having the k parity-check bits set at positions 1; 2; : : : ; 2_{k-1} and checking every element whose binary representation has a "1" in position $k_{i\ -1}$. Encoding a message in this manner is computationally simple and understandable. Decoding it and determining where there is an error turns out to be just as Simple. Hamming codes have one distinct problem. They are relatively inefficient when sending small amounts of data, but they get increasingly inaccurate as the number of bits increases.

Reed-Muller codes are described as R(r;m), where m is the number of spanning vectors (causing the space to have 2m dimensions) and r is the depth of linear combinations of spanning vectors. This code create a polynomial using thedata bits as the coefficients for the spanning vectors. The oversampled section of this polynomial are sent. The original polynomial can be reconstructed by multiplying the data points with vectors perpendicular to the spanning vectors. Then, the original data can be reconstructed. Reed-Muller codes are designed to only handle binary representation. The larger the code word, the more errors this code can correct. The encoding and decoding algorithm is significantly more complexthen the Hamming Code. Reed-Muller codes

Low-density parity-check (LDPC) codes are encodings that use specific parity bits[2]. They are designed in such a way that all bits act equivalently. Each parity-check bit checks some small fixed k ϵ Z bits and each bit is checked by some small fixed j ϵ Z parity-check bits. LDPC codes were also very erratic in how

effectively they worked and there was no computationally feasible methods for creating effective ones.

Convolution codes encode bits based upon a state which is determined by summing a fixed set of previously bits. Each input bit is manipulated in a few different ways to produce several outputs bits. Therefore each output bit conveys the combined information of many different input bits. The state is initialized to a key that is initially passed from encoder to decoder. Due to the integral part this key plays in decoding, these codes are often used for cryptography. Convolution codes are significantly better at approaching the theoretical Shannon limit then prior error correcting codes. They are fast, efficient and generally accurate. Unfortunately their accuracy varies significantly depending on the input. In specific, convolution codes have specific codewords where their accuracy plummets.

The simplest turbo codes work through a series of simultaneous steps. The input is split into as many copies as desired. Then a copy is sent directly through a convolution code. Simultaneouslyanother copy is permuted and sent through a potentially different convolution code. This process is repeated using different permutations and potentially different convolution codes until all the copies are sent. Turbo codes are most effective on longer codewords and are consistently close to Shannon's limit.

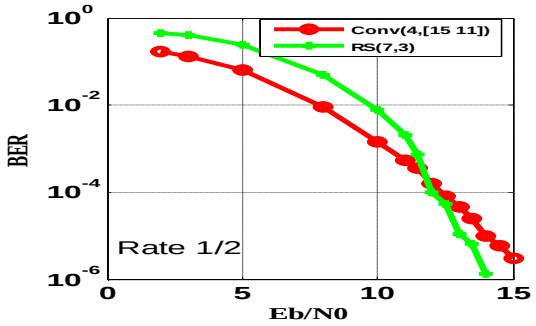

Fig.1 Comparison of Rs(7,3)(Rate 1/2) and Conv(4,[15 11])(Rate 1/2)

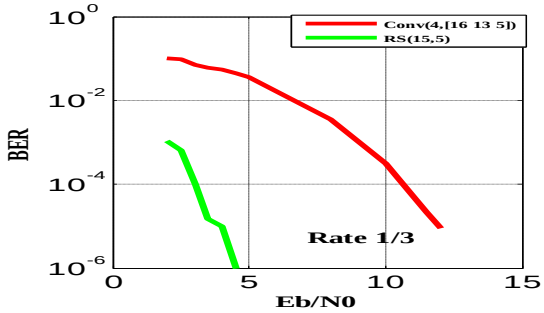

Fig.2 Comparison of Rs(15,5)(Rate 1/3) and Conv(4,[16 13 5])(Rate 1/3)

For Reed Solomon codes required Eb/N0 for specific BER is much less than Eb/N0 required for convolution codes

reed solomon codes

Architecture:

Error detection is the detection of errors caused by noise or other impairments during transmission from the transmitter to the receiver. Error correction is the detection of errors and reconstruction of the original, error-free data. Error-correcting codes are usually distinguished between convolution codes and block codes:

Convolution codes are processed bit-by-bit. Block codes are processed block-by-block. Early examples of block codes are repetition codes, Hamming codes and multidimensional parity-check codes. They were followed by a number of efficient codes, Reed-Solomon codes being the most notable due to their current widespread use. Reed Solomon codes are linear block codes and a subset of BCH codes[4]. A Reed-Solomon code is specified as RS(n,k) with s-bit symbols where k is the number of information bits and n is the length of total codeword. 2t parity symbols are added to make an n symbol codeword. A Reed-Solomon decoder cancorrect up to t symbols that contain errors in a codeword, where 2t = n-k.

The following diagram shows a typical Reed-Solomon codeword. This is known as a Systematic code because the data of k symbols is left unchanged and the 2t parity symbols are appended at the end.

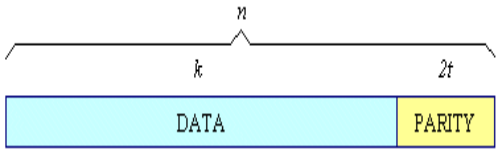

Figure3: Reed Solomon Codeword

The maximum codeword length (n) for a Reed-Solomon codeisn=2s– 1…… (1)

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 Advantages of Reed Solomon w.r.t. other block codes are:

a. The systematic format

b.The efficient encoding and decoding algorithm

c.The powerful error correction capability

d.Good for handling burst-errors (using symbols and not bits)

e.Does not require a back-channel (as opposed to ARQ). Therefore, an excellent solution for multicast

Proposed tools:

VHDL: VHDL stands for VHSIC (Very High Speed Integrated Circuits) Hardware Description Language. A hardware description language is inherently parallel, i.e. commands, which correspond to logic gates, are executed (computed) in parallel, as soon as a new input arrives.

Matlab: MATLAB (matrix laboratory) is a numerical computing environment and fourth-generation programming language. Developed by MathWorks, MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, and Fortran.

SPICE: SPICE is a general-purpose open source analog electronic circuitsimulator. It is a powerful program that is used in integrated circuit and board-level design to check the integrity of circuit designs and to predict circuit behavior.

PROPOSED MODEL

One typical application of the RS codes is the Forward Error Correction (FEC), shown in Fig.3

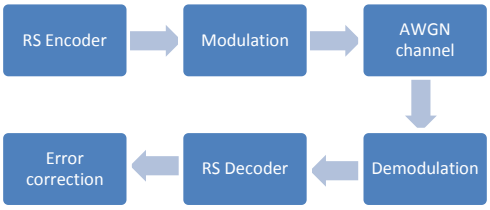

Fig.4 System model

Before data transmission, the encoder attaches parity symbolsto the data using a predetermined algorithm before transmission. At the receiving side, the decoder detects and corrects a limited predetermined number of errors occurred during transmission. Transmitting the extra parity symbols requires extra bandwidth compared to transmitting the pure data. However, transmitting additional symbols introduced by FEC is better than retransmitting the whole package when at least an error has been detected by the receiver.

Encoder:

The concept of Reed-Solomon coding describes encoding of k message symbols by viewing them as coefficients of a polynomial m(x) of maximum degree k-1 over a finite field of order N. Then evaluating the polynomial at n>k distinct input points. Sampling a polynomial of degree k-1 at more than k points creates an overdetermined system.

In practice, instead of sending sample values of a polynomial, the encoding symbols are viewed as the coefficients of an output polynomial C(x) constructed by multiplying the message polynomial m(x) of maximum degree k-1 by a generator polynomial g(x) of degree t=N-k-1.

k = No. of information symbols
n= No.of symbols in encoded codeword
m(x)= message polynomial
g(x)= generator polynomial
C(x)= output polynomial
R(x)=received polynomial
α=Root of primitive polynomial

The generator polynomial g(x) is defined by having α, α2, ..., αt as its roots, i.e.,

$$g(x) = (x+\alpha)(x+\alpha^2)(x+\alpha^3)(x+\alpha^4).....(x+\alpha^{2t}) \quad \ldots..(2)$$

The transmitter sends the N-1 coefficients of C(x) = m(x)g(x).

Modulation and demodulation:

In digital communication different modulation techniques can be used for different kind of data. Since Reed Solomon codes are not binary codes and they work on integer numbers as input all modulation techniques can not be applied. In this paper PSK and QAM modulation techniques are compared.

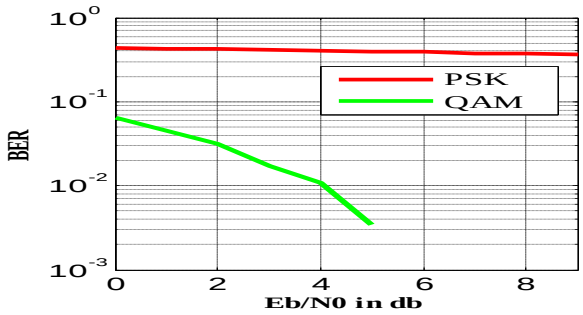

Fig.5 PSK modulation vs QAM modulation

Channel :

Additive white Gaussian noise (AWGN)Introduces white noise at all frequencies. Rician channel is a transmission channel that may have a line-of-sight component and several scattered of multipath components. Rayleigh fading is caused by multipath reception. In this section AWGN and Rician channel response is compared.

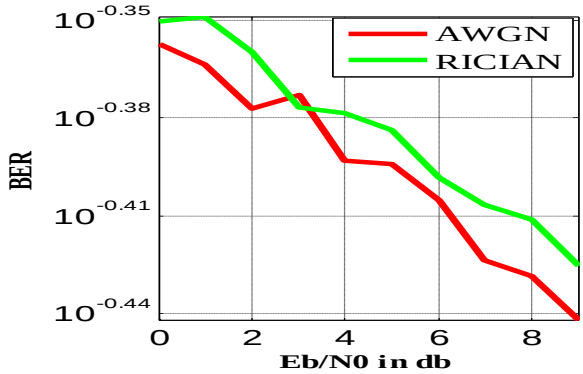

Fig.6 Psk awgn vs psk rician

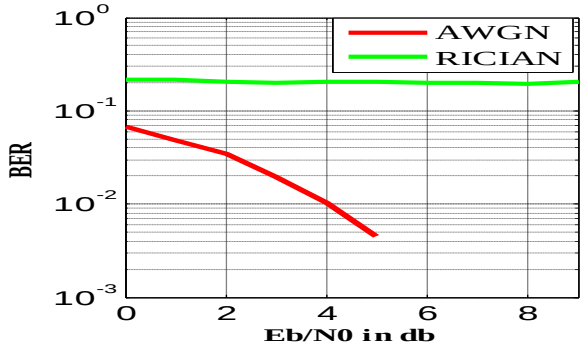

Fig.7 QAMAWGN vs QAMRician

RS Decoder:

The RS decoding algorithm can be mainly divided into two classes: time domain and frequency domain. Because it requires extra error value transformation block, inverse transformation block and delay block for syndrome polynomial, the dissipation and chip area of frequency-domain decoding algorithm is greater than that of time

domain. Therefore, in this paper, the time-domain decoding algorithm is chosen.

The time-domain decoding algorithm can be divided into two main classes according to methods to solve error locator polynomial: Berlekamp-Massey (BM) algorithm and Euclideanalgorithm. The former one has an advantage on implementation complexity while the latter one has less critical-path delay. the Euclidean algorithm has simpler structure than the BM algorithm does. However, it needs a significant amount of logicelements to implement the polynomial division function. On the other hand, the BM algorithm has a complex structure, butuses fewer gates to be implemented.

I. RS CODE FOR DIFFERENT R AND DIFFERENT T:

The BER vs. Eb/No curves have been obtained by simulation for several codes over GF(28) with the same rate R=0.8.

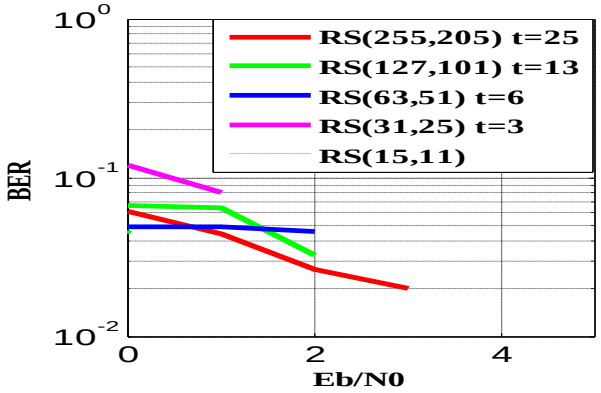

Fig.8 RS codes with R=0.8

Figure shows that for higher values of n and k BER is less. This concludes that for better performance of RS codes higher values of n and k should be chosen.

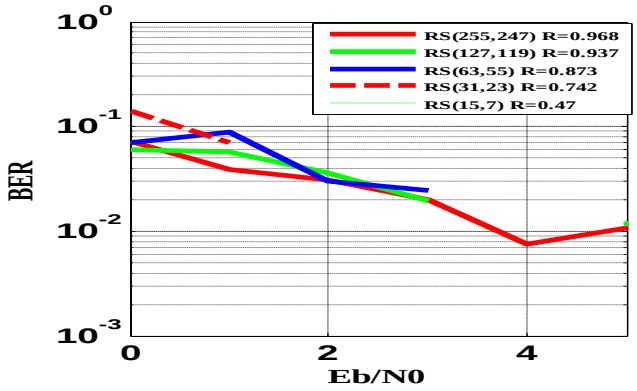

Fig.9 RS codes with t=4

Figure 6 shows that for higher values of t, BER is less but computational complexity increases. There is a trade of between lower values of t and performance of RS codes[5]. But from figure 6 it is clear that effect of R on performance is preponderant compared to effect of t. Hence this section can conclude that to improve computational complexity low value for t should be chosen. For better performance of the system higher values of n and k should be chosen.

II. RESULTS AND DISCUSSION:

Encoder output:

Generator polynomial for RS(7,3):

1 + 3 X + X2 + 2 X 3 + 3 X 4

For input m1= 1 + X 2

Output of encoder is C1:

1 + 3 X + 2 X2 + 5 X3 + 4 X4 + 2 X5 + 3 X6

For onput m2= 1 + X

Output of encoder is C2:

1 + 4 X + 4 X2 + 3 X3 + 5 X 4 + 3 X5

A matlab code is written for RS encoder and codeward is generated for two different generator polynomials.

BER for RS(255,247):

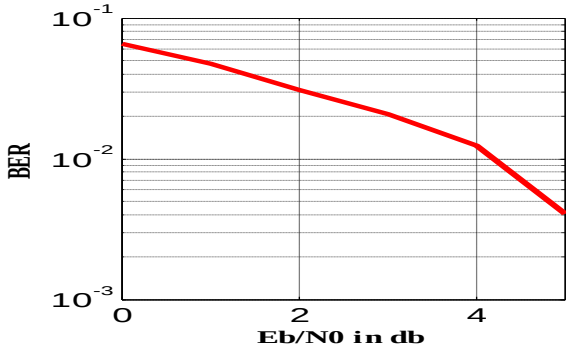

Fig.10RS(255,247)

Using matlab code for RS code , BER of the system is found to be in between 10^{-3}

Simulink model for Reed Solomon code:

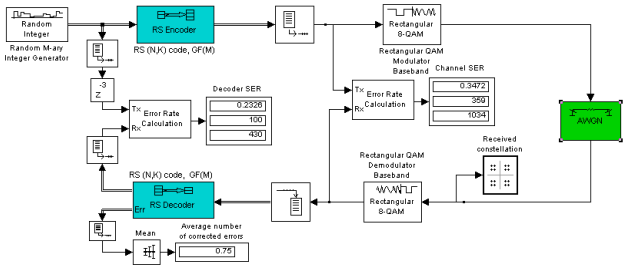

Fig.10 Simulink model

A matlab simulink model is designed for RS(7,3) and RS(255,247).

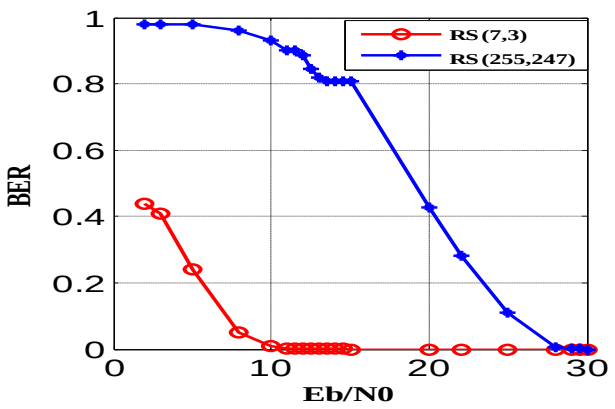

Fig.11 Simulink model results

It is found that for RS(7,3) , BER 0f 1.6x10-6 is achieved at 14.5 db and for RS(255,247), BER 0f 7.8x10-6 is achieved at 29.6 db .It is found that simulink model is giving better BER compared to matlab program.

CONCLUSION:

Reed Solomon is good for handling burst errors. It is widely used in applications such as storage, satellite, digital TV etc. It is a noble idea to implement it using a reconfigurable device like FPGA. This paper proposes an illustration of RS(7,3) and RS(255,247). The same architecture will be implemented on RS(n,k), where n and k can vary. The same architecture is simulated using matlab simulink model and it is observed that a BER of 10-6 is achieved. In future it can be implemented using Xilinx,s SpartranIII device and the results can be compared with other FPGA devices. Similarly it can be implemented using Matlab cosimulation.

REFERENCES:

[1] S. B. Wicker Error control systems for digital communication and storage, Prentice hall, 1995.

[2] Gallager, Robert G. ”Low-Density Parity-Check Codes” pp. 1-20. Monograph,M.I.T. Press, 1963.

[3] Hamming, R.W. ”Error Detecting and Error correcting Codes”, The Bell SystemTechnical Journal,J Soc, Indust. Appl. Math. Vol. 26, No.2, April 1950.

[4] Reed, I. S. and Solomon, G. ”Polynomial Codes Over Certain Finite Fields”, JSoc, Indust. Appl. Math. Vol. 8, No. 2, June 1960.

[5]Lionel Biard, Dominique Noguet “Choice and Implementation of A Reed Solomon code for Low PowerLow Data Rate Communication Systems” IEEE Radio and Wireless Symposium, 2007 .

[6] Kan, M.; Okada, S.; Maehara, T.; Oguchi, K.; Yokokawa, T.; Miyauchi, T.,” Hardware implementation of soft decision decoding for Reed Solomon Code”, Turbo Codes and Related Topics, 2008 5th International Symposium on Digital Object Identifier.

[7] Brauchle, J.; Koetter, R.” A Systematic Reed Solomon Encoder with Arbitrary Parity Positions’, IEEE Global Telecommunications Conference, 2009. GLOBECOM 2009.

[8] Mursanto, P.” Performance Evaluation of Galois Field Arithmatic Operators for Optimizing Reed Solomon Codec”,Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME), 2009 International Conference on Digital Object Identifier.

[9] McSweeney, R.; Spagnol, C.; Popovici, E.” ComparativeStudy of Software Vs. Hardware Implementations of Shortened Reed Solomon Code for Wireless Body Area Networks”, Microelectronics Proceedings (MIEL), 2010, 27th InternationalConference on Digital Object Identifier.

[10] Meng Zhang, Xing Gao, Zhisheng Dai, Tingting Tao, Zhongju Yin, Shengli Lu “VLSI Implementation and Optimization Design of Reed-Solomon Decoder in QAM Demodulation Chip” Circuits and Systems, 2008. APCCAS 2008. IEEE Asia Pacific Conference on Digital Object Identifier: 10.1109/APCCAS.2008.4746359