Review paper on Reed Solomon (204,188) Decoder for Digital Video Broadcasting – Terrestrial application

Snehal Jawanjal[1], Shrikant Bhoyar[2], Pooja Hatwar[3], Rahul Sathawane[4]

[1] *Asst. Prof., Department of ETX, RGCER, Nagpur, Maharashtra, India*
[2] *Asst. Prof., Department of ETX, RGCER, Nagpur, Maharashtra, India*
[3] *M. Tech. Scholar, Department of ETX, RGCER, Nagpur, Maharashtra, India*
[4] *Asst. Prof., Department of IT, RGCER, Nagpur, Maharashtra, India*

***

Abstract - *Reed-Solomon (RS) codes are commonly used in the digital communication field due to their strong capabilities to eliminate both random errors and burst errors. In this paper, the encoding and decoding systems of a (204, 188) Reed-Solomon code is being studied and observed. Reed-Solomon codes are used to perform Forward Error Correction. FEC encoders introduce redundancy in data before it is transmitted. The redundant data (check symbols) are transmitted along with the original data through the channel. A Reed-Solomon decoder at the receiver is used to recover any corrupted data This type of error correction is widely used in data communications applications such as hard disk and media storage (CD) systems, Digital Video Broadcast (DVB) and Optical Carriers (e.g. OC-192).*

Key Words: *Reed Solomon (RS), random errors, burst errors, FEC, redundant data, Reed-Solomon decoder, DVB*

1. INTRODUCTION

The concept of communication system is the sum of all the systems and devices that are involved in information transmission. Communication system can be generally divided into two classes based on the different types of signals that are transmitted. One is digital communication system and the other is analog communication system. Enjoying the benefit that it is amenable to both error control and encryption, digital communication system is more often used nowadays. In communication systems, information is transmitted through physical media which are channels. Since channels cannot avoid the interference from the outside world, the transmitted information will be distorted which ultimately results in errors in the received information. Therefore, error control is employed to help optimize the accuracy and reliability of the transmission and advance the distortion resistance capability of the channel. Error control is a method that can detect and correct errors. Generally, there are two patterns of error control: the first one is that once errors are detected, the decoder automatically corrects these errors based on certain rules; another method is that once errors occur, instead of correcting the errors, the receiving end sends a feedback signal to the transmitting end telling it that errors occurred and requests that message to be sent again.

1.2 Reed Solomon codes

Finite field or Galois field is an algebraic theory raised by French mathematics genius Évariste Galois. Galois fields are very important in coding theory. The Reed-Solomon codes studied in this paper are based on finite fields. If the number of elements on a field F is finite, this field is called a finite field, or a Galois field. The number of elements is called the order of the field. Galois field F = {0 1, 2, …, -1} is a finite field with modulus p and order p and it can be represented as GF (p). Number p is a prime number. A polynomial over a field is a polynomial of which the coefficients are the elements of a Galois field GF(p). The polynomial over GF(p) is represented as

$$p(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_p x^p ;$$
$$\text{in which } a_i \in F,\ i = 0, 1, 2, \dots, p.$$

A Reed Solomon code is a block code, meaning that the message to be transmitted is divided up into separate blocks of data. Each block then has parity protection information added to it to form a self-contained code word. It is also a systematic code, which means that the encoding process does not alter the message symbols and the protection symbols are added as a separate part of the block.

Also, a Reed Solomon code is a linear code(adding two code words produces another code word) and is cyclic(cyclically shifting the symbols of a code word produces another code word). It belongs to the family of Bose-Chaudhari-Hocquenghem(BCH) codes, but is distinguished by having multi-bit symbols. Thus a Reed Solomon code can be described as an (n,k) code, where n is the block length in symbols and k is the number of information symbols in the message.

2. THE RS ENCODER

The encoding procedures of RS codes are similar as the encoding of general cyclic codes. Let the message bits M be

$$M = (m_k , m_{k-1}, m_1).$$

The information polynomial m(x) is

$$m(x) = m_k x^{k-1} + m_{k-1} x^{k-2} + \dots\dots m_x x + m_1.$$

The code word C is

$$C = (c_n , c_{n-1} , \dots\dots c_1).$$

The code word polynomial c(x) of the RS code is

$$c(x) = c_n x^{n-1} + c_{n-1} x^{n-2} + \dots\dots c_2 x + c_1 .$$

The generator matrix g(x) of the RS code is

$$g(x) = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{2t}).$$

The encoding steps are

(1) Multiply the information polynomial m(x) by x^{n-k} ;

(2) Divide m(x) x^{n-k} by g(x) to obtain the remainder r(x), i.e.

$$r(x) = m(x)\ x^{n-k} \bmod g(x);$$

(3) Derive code word polynomial c(x) through m(x) and r(x), i.e.

$$c(x) = m(x)\ x^{n-k} + r(x).$$

Through the above three steps, the code word of a RS code is generated as

$$C = (c_n , c_{n-1} , \dots\dots c_1)$$

$$= (m_k , m_{k-1}, \dots\dots m_1, r_{n-k} , \dots\dots r_1).$$

The first k symbols are information symbols and the last r=n-k symbols are parity check symbols. This algorithm is called the time-domain algorithm of RS code and the code obtained is called systematic code.

3. THE RS DECODER

The code word c(x) obtained after encoding will be interfered when transmitted in the channel. Let the noise be e(x), i.e. error pattern. It will be added onto c(x) and the sum will be transmitted to the receiver. Let the polynomial of the received vector be r(x), then r(x) = c(x) + e(x). The expressions of c(x), e(x), and r(x) are given below

$$c(x) = c_0 + c_1 x + c_2 x^2 + \dots\dots c_{n-1} x^{n-1} .$$

$$e(x) = e_0 + e_1 x + e_2 x^2 + \dots\dots e_{n-1} x^{n-1} .$$

$$r(x) = r_0 + r_1 x + r_2 x^2 + \dots\dots r_{n-1} x^{n-1} .$$

The basic decoding theory of a RS code is to derive the error pattern e(x) based on the received vector r(x), and then obtain code word c(x) according to equation r(x) = c(x) + e(x).

Decoding methods can be divided into two categories. One is time domain decoding and the other is frequency domain decoding. Time domain decoding is to locate the errors based on the received vector and it does not need transform calculation. Frequency domain decoding is to obtain the error location by perform Fourier transform. Since it is easier to apply, this dissertation employs time domain decoding.

The steps of time domain decoding are described as below:

1) Find out the syndrome s(x) and the key equation using the received signal r(x).

2) Determine error location polynomial σ(x) and the error-value evaluator polynomial ω(x) based on the syndrome s(x).

3) Determine the error location number x_i using Chien search.

4) Evaluate error-value polynomial y_i according to σ(x) and x_i.

5) Obtain the information sequence based on r(x) and y_i.

3.1 Syndrome calculator

The first step in decoding the received symbol is to determine the data syndrome. 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 syndrome polynomial is generally represented as,

$$s(x) = s_1 + s_2 x + s_3 x^2 + \ldots + s_{2t} x^{2t-1}$$

$$= \sum_{j=0}^{n-1} r_j (a_i)^j$$

Where, α is the primitive element.

If si = 0, the transmission is error-f ; f s≠0, s occurred in the transmission, and the error pattern needs to be determined to perform error correction

3.2 Error-Locator Polynomial

The next step, after the computing the syndrome polynomial is to calculate the error values and their respective locations. This stage involves the solving of the 2t syndrome polynomials, formed in the previous stage. These polynomials have ‗v' unknowns, where v is the number of unknown errors prior to decoding. If the unknown locations are
(i1,i2,……iv,) the error polynomial can be expressed as,

$$E(x) = Y_1 x^{i_1} + Y_2 x^{i_2} + \ldots + Y_v x^{i_v}$$

Where Yl is the magnitude of the lth error at location il. If Xl is the field element associated with the error location il, then the syndrome coefficients are given by,

$$S_j = \sum_{l=1}^{v} Y_l x_l^j$$

Where, j=1,2,….,2t. And Yl is the error value and Xl is the error location of the lth error symbol. The expansion of (4.8) gives the following set of 2t equations in the v unknown error locations X1, X2, ... Xv and ‗v' unknown error magnitudes Y1 ,Y2 ,......Yv.

$$S_1(x) = Y_1 X_1 + Y_2 X_2 + \ldots + Y_v X_v$$

$$S_2(x) = Y_1 X_1^2 + Y_2 X_2^2 + \ldots + Y_v X_v^2$$

$$\vdots$$

$$S_{2t}(x) = Y_1 X_1^{2t} + Y_2 X_2^{2t} + \ldots + Y_v X_v^{2t}$$

The above set of equations must have at least one solution because of the way the syndromes are defined. This solution is unique. Thus the decoder‘s task is to find the unknowns given the syndromes. This is equivalent to the problem in solving a system of non-linear equations. Clearly, the direct solution of the system of nonlinear equations is too difficult for large values of v. Instead, intermediate variables can be computed using the syndrome coefficients Sj from which the error locations, X1, X2 ,......., Xv , can be determined. The error-locator polynomial is introduced as

$$\sigma(x) = \sigma_v x^v + \sigma_{v-1} x^{v-1} + \ldots + \sigma_1 x + 1$$

The polynomial is defined with roots at the error locations −1 i.e Xl-1 for l=1,2,…v. The error location numbers l, X indicate errors at locations il for l=1, 2, …v This can be written as,

$$\sigma(x) = (1 - xX_1)(1 - xX_2) \ldots (1 - xX_v)$$

Where, Xl =αil

3.3 Chien Search

The roots obtained will now point to the error locations in the received message. RS decoding generally employs the Chien search scheme to implement the same. A number ‘n‘ is said to be a root of a polynomial, if the result of substitution of its value in the polynomial evaluates to zero. Chien Search is a brute force approach for guessing the roots, and adopts direct substitution of elements in the Galois field, until a specific i from i=0, 1,.., (n-1) is found such that σ (αi) = 0 . In such a case αi is said to be the root and the location of the error is evaluated as σ(x). Then the number of zeros of the error locator polynomial σ(x) is computed and is compared with the degree of the polynomial. If a match is found the error vector is updated and σ (x) is evaluated in all symbol positions of the codeword. A mismatch indicates the presence of more errors than can be corrected.
Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here. Paragraph comes content here.

4. Digital Video Broadcasting

Digital television (DTV) broadcasting is in the process of migrating from analog to digital systems, with regions around the world at different stages of adoption. Various delivery systems are available for digital TV, but the main ones are satellite, cable, terrestrial, and mobile. Each has a variety of standards and derivatives that are either mature or emerging. These standards aim to ensure interoperability between different vendor’s equipment, including the set-top boxes, cell phones, and other means for DTV reception. The DVB-T system is the terrestrial transmission system of the DVB standards. For error protection, a concatenated forward error correction (FEC) scheme is used. The randomized packets are encoded by the Reed-Solomon (R-S) Encoder using a (*n, k*) code; where *n* is the block size and *k* is the number of information symbols. In this case, *n* is 204 symbols and *k* is 188 symbols, and a symbol represents 8 bits. This means that 16 check symbols are appended to the information bytes. This code allows up to 8 symbols of data to be corrupted and still be corrected, that is a total of 64 bits.

5.EXPECTED OUTCOME

In this paper an introduction to the theory of error controls coding and fundamentals of finite field will be presented. Then, the (204, 188) Reed Solomon encoder / decoder systems is to be designed, simulated and verified to detect the errors. We may observe the following characteristics:

- Code length: n = 204.
- Information symbols: k = 188.
- Parity check symbols: r = n – k =16.
- Minimum distance: dmin = n – k + 1 = 17.
- Error correcting capability: t = 8

REFERENCES

[1] P.Sunitha ;G.V.Ujwala " Implementation of Reed Solomon Encoding Algorithm" International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056 Volume: 02 Issue: 06, Sep-2015 p-ISSN: 2395-0072

[2] Aqib Al Azad and Md Imam Shahed, —A Compact and Fast FPGA Based Implementation of Encoding and Decoding Algorithm Using Reed Solomon Codes||, International Journal of Future Computer and Communication, vol.2, no. 6, pp.- 31-35, February 2014.

[3] Xiaojun Wu; Xianghui Shen; Zhibin Zeng "An improved RS Encoding Algorithm" Consumer Electronics Communications and Networks (CECNet), 2012 2nd International Conference on Digital Object Identifier, Page(s): 1648 – 1652.

[4]Yung-Kuei Lu; Ming-Der Shieh "Efficient Architecture for Reed-Solomon Decoder" VLSI Design, Automation, and Test (VLSI-DAT), 2012 International Symposium on Digital Object Identifier, Page(s): 1 – 4.

[5]Al Azad, Minhazul. Huq, Iqbalur. Rahman Rokon "Efficient Hardware Implementation of Reed Solomon Encoder and Decoder in FPGA using Verilog" International Conference on Advancements in Electronics and Power Engineering (ICAEPE'2011) Bangkok Dec. 2011

[6] Hsie-Chia Chang, Chih-Yu Cheng, Shu-Hui Tsai, and Chen-Yi Lee , "A (204,188) Reed-Solomon Decoder using Decomposed Euclidean Algorithm", Roc. 43rd IEEE Midwest Symp. on Circmts and Systems, Lansing MI, Aug 8-2011, 200862.

[7] Richard Huynh, GE Ning & YANG Huazhong, "A Low Power Error Detection in the Syndrome Calculator Block for Reed-Solomon Codes: RS(204,188)", TSINGHUA SCIENCE AND TECHNOLOGY ISSNll1007-0214ll09/19llpp474-477 Volume 14, Number 4, August 2009.

[8]Zhigang Ren; Dongping Yao "An Improved High-speed RS Encoding Algorithm" Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2009 3rd IEEE International Symposium on Digital Object Identifier, Page(s): 521 – 523.

[9] Anne Franssens, "Analysis of Reed Solomon error correcting codes on reconfigurable hardware", Thesis from University of Twente, Enschede, The Netherlands, September 9, 2008.

[10] Priti Shankar, "Decoding Reed–Solomon Codes Using Euclid's Algorithm", General article in Resonance, April 2007.

[11] "Digital Video Broadcasting (DVB); Framing Structure, Channel Coding and Modulation for Digital Terrestrial Television", ETSI EN300 421, V1.5.1, Jun. 2004.

[12] Kim Hamilton,"Polynomial Codes over Certain Finite Fields" by Irving Reed and Gustave Solomon, presented in March 2003.

[13] C.K.P. Clarke, "Reed Solomon error correction", R&D White paper, July 2002.