Journal of Basic and Applied Engineering Research
Print ISSN: 2350-0077; Online ISSN: 2350-0255; Volume 2, Number 10; April-June, 2015 pp. 839-841
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/jbaer.html

Design of Galois Field Multiplier for RS(15,11) Encoder

Snehal.P.Jawanjal[1], S. R.Bhoyar[2] and Ashwini Raut[3]

[1,2,3]Electronics Engineering Department Rajiv Gandhi College of Engg. & Research, Nagpur, India
E-mail: [1]jawanjal.snehal@gmail.com, [2]shrikantbhoyar08@gmail.com, [3]raut.ashu87@gmail.com

Abstract—*Reed Solomon error correction has several applications in broadcasting,in particular forming part of the specification for the digital terrestrial television standard known asDVB-T.*
Hardware implementation for coders and decoders for Reed Solomon error correction are complicated and require some knowledge of the theory of the Galois field on which they are based.This paper present the underlying mathematics and algorithm used for coding and decoding with particular emphasis on their realization in logic circuits..

Keywords: *Galois Field arithmatic, Error Correcting codes,DVB-T Reed solomnon,Two parallel RS encoder, XOR optimization, generator polynomial .*

1. INTRODUCTION

Many digital sampling applications in broadcasting use Forward error correction a technique in which redundant information is added to the signal to allow the receiver to detect and correct errors that may have occurred during transmission.

Reed Solomon codes are a particular case of non-binary BCH codes. They are extremelypopular because of their capacity to correct burst errors. Their capacity to correct burst errors stems from the fact that they are word oriented rather than bit-oriented. A bit-oriented code such as a BCH code would treat this situation as many independent single-bit errors. To a Reed Solomon code, however a single error means any or all-incorrect bits within a single word. Therefore the RS (Reed Solomon) codes are designed to combat burst errors in a channel. Infact RS codes are a particular case of non-binary BCH codes.

2. REED SOLOMON

The structure of a Reed Solomon code is specified by the following two parameters:

- The length of the code-word m in bits,often chosen to be 8,
- The number of errors to correct T.

A code-word for this code then takes the form of a block of m bit words. The number of words inthe block is N, which is always equal to N = 2m – 1 words, of which 2T words are parity or checkwords. For example, the m = 8, t = 3 RS code uses a block length of N = 255 bytes, of which 6are parity and 249 are data bytes. The number of data bytes is usually referred to by the symbolK. Thus the RS code is usually described by a compact (N,K,T) notation. The RS codediscussed above for example has a compact notation of (255,249,3). When the number of data bytes to be protected is not close to the block length of N defined by N = 2m – 1 words atechnique called shortening is used to change the block length. A shortened RS code is one inwhich both the encoder and decoder agree not to use part of the allowable code space. Forexample, a (204,188,8) code would only use 204 of the allowable 255 code words defined by them = 8 Reed Solomon code. An error correcting code, such as an RS code, is said to besystematic if the user data to be encoded appears verbatim in the encoded code word. Thus a systematic (204,188,8) code would have the 188 data bytes provided by the user appearing verbatim in the encoded code word, appended by the 16 parity words of the encoder to form one block of 204 words. The choice of using a systematic code is merely from the point of simplicity as it lets the decoder recover the data bytes and strip off the parity bytes easily, because of the structure of the systematic code.

3. GALOIS FIELD

A field is a set of elements on which two binary operations can be performed. Addition andmultiplication must satisfy the commutative, associative and distributive laws. A field with a finitenumber of elements is a finite field. Finite fields are also called Galois fields after their inventor. An example of a binary field is the set {0,1} under modulo 2 addition and modulo 2multiplication and is denoted GF(2). The modulo 2 addition and subtraction operations aredefined by the tables shown in the following figure. The first row and the first column indicate theinputs to the Galois field adder and multiplier.

For e.g. 1 + 1 = 0 and 1 * 1 = 1.

In general if p is any prime number then it can be shown that GF(p) is a finite field with p elementsand that GF(pm) is an extension field with pm elements. In addition the various elements of thefield can be generated as various powers of one field element a, by raising it to different powers.For example GF(256) has 256 elements which can all be generated by raising the primitiveelement 2 to the 256 different powers.

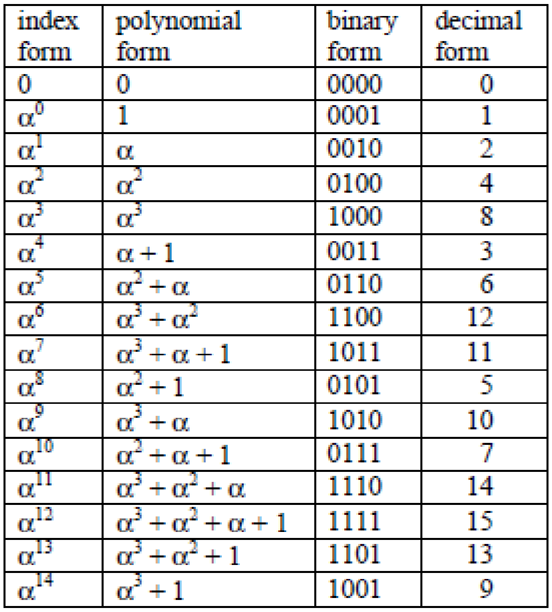
In addition, polynomials whose coefficients are binary belong to GF(2). A polynomial over GF(2)of degree m is said to be irreducible if it is not divisible by anypolynomial over GF(2) of degreeless than m but greater than zero. The polynomial F(X) = X2 + X + 1 is an irreducible polynomialas it is not divisible by either X or X + 1. An irreducible polynomial of degree m which dividesX2m–1 + 1, is known as a primitive polynomial. For a given m, there may be more than oneprimitive polynomial. An example of a primitive polynomial for m = 8, which is often used in mostcommunication standards is F(X) = 1 + X^2+ X^3+ X^4+ X^8.

The primitive polynomial,

$$p(x)=x^4+x+1 \qquad (1)$$

For GF with the field generator polynomial shown in (1),we can write,

$\alpha^4+\alpha+1$



index form	polynomial form	binary form	decimal form
0	0	0000	0
α^0	1	0001	1
α^1	α	0010	2
α^2	α^2	0100	4
α^3	α^3	1000	8
α^4	$\alpha+1$	0011	3
α^5	$\alpha^2+\alpha$	0110	6
α^6	$\alpha^3+\alpha^2$	1100	12
α^7	$\alpha^3+\alpha+1$	1011	11
α^8	α^2+1	0101	5
α^9	$\alpha^3+\alpha$	1010	10
α^{10}	$\alpha^2+\alpha+1$	0111	7
α^{11}	$\alpha^3+\alpha^2+\alpha$	1110	14
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111	15
α^{13}	$\alpha^3+\alpha^2+1$	1101	13
α^{14}	α^3+1	1001	9

Fig. 1: The field elements for GF(16)with p(x)=x^4+x+1

$Z_3=a_3b_3+a_3b_0+a_2b_1+a_0b_3+a_1b_2$

$Z_2=a_3b_3+a_3b_2+a_2b_3+a_2b_0+a_1b_1+a_0b_2$

$Z_1=a_3b_2+a_2b_3+a_3b_1+a_2b_2+a_1b_3+a_1b_0+a_0b_1$

$Z_0=a_3b_1+a_2b_2+a_1b_3+a_0b_0$

For constant =15,

Z3=b0+b1+b2

Z2=b0+b1

Z1=b0

Z0=b0+b1+b2+b3

For constant =3,

Z3=b3+b2

Z2=b1+b2

Z1=b3+b0+b1

Z0=b0+b3

For constant =1,

Z3=b3

Z2=b2

Z1= b1

Z0=b0

For constant =12,

Z3=b3+b0+b1

Z2=b0+b2

Z1=b3 +b1

Z0=b1+b2

Table 1: Comparison between Generalised and Constant Optimized Multiplier

No. of Gates reuired	Generalised Multiplier	Constant (15)Optimized Multiplier
AND Gate	22	0
XOR Gate	18	6

4. CONCLUSION

The number of AND gates are completely reduced when Galois field multiplier is optimized using constant.Hence for entire architecture required no. of XOR gates are less.

REFERENCES

[1] Jittawukipoka and Ngarmnil IEEE “Low complexity Reed Solomon Encoder Using Globally Optimized Finite Field multipliers” TENCON 2004, IEEE Region 10, Vol. 4, pp. 423-426, Nov . 2004.

[2] Chang-Seok CHOI, Hyo-Jin AHN and Hanho LEE, “High-Throughput Low –Complexity Four-Parallel Reed-Solomon Decoder Architecture for High-Rate WPAN systems” IEICE, TRANS. ON COMMUNI., VOL. E94-B,NO.5 MAY 2011

[3] Chang-Seok Choi and Hanho Lee, “ High Speed Low Complexity Three Parallel Reed Solomon Decoder for 6-gbps mmWave WPAN systems”. European Conference on Ciruit theory and Design 2009 (ECCTD’ 2009), pp 515-518, Aug. 2009 .

[4] Aqib.Al Azad,Minhazul.huq, Iqbalur, Rahman Rokon, “Efficient Hardware Implementation of Reed Solomon Encoder and Decoder in FPGA using Verilog” ICAEPE’2011 Bangkok DEC.,2011.

[5] Christof Paar, “Optimized arithmetic for Reed-Solomon Encoders”, 1997 IEEE International Symposium on Information Theory, June 1997.