American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-7, Issue-2, pp-110-116
www.ajer.org
Research Paper Open Access

Minimized Logic Gates Number Of Components In The Chien Search Block For Reed-Solomon (RS)

Elghayyaty Mohamed[1], Hadjoudja Abdelkader[2], Omar Mouhib[2], El Habti El Idrissianas[2], Mahjoub Chakir[1]

[1](Laboratory of engineering Sciences and modeling. Faculty of Sciences, University Ibn Tofail Kenitra, Morocco

[2](Laboratory of Electrical Engineering and Energy System. Faculty of Sciences, University Ibn Tofail Kenitra, Morocco

Corresponding author: Elghayyaty Mohamed

Abstract: *A Reed-Solomon (RS) code is an error-correcting code first described in a paper by Reed and Solomon in 1960.Since that time they've been applied in CD-ROMs, wireless communications, space communications, DSL,DVD, and digital TV.RS encoding data is relatively straightforward, but decoding is time- consuming, despite major efficiency improvements made by Berlekamp and other during the 1960' .Only in the past few years has it become computationally possible to send high-bandwidth data using RS.*

RS differs from a Hamming code in that it encodes groups of bits instead of one bit at a time.We will call these groups "digits" (also "symbols" or "coefficients").A digit is error-free if and only if all of its bits are error-free. For instance, if a digit is an 8-bit character, and three bits of the same single character are in error,we ill count that as one corrupted digit.

Keywords*: Reed-Solomon Coding, Chien Search Block, Error detection, factorization method, minimized logic gates, VHDL.*

I. INTRODUCTION

The development of the use of computers and digital technology in our societies poses the problem of the transmission of digital information, the main criterion of a good transmission being the preservation of the integrity of the initial information at the end of the transmission process of it. The role of error-correcting codes is to ensure the accuracy of the information we access. The constant increase in the use of digital technology in our society makes these all the more important. Several common examples illustrate this problem: a first is the transmission of a message via the Internet, where the message can be altered because of the noise on the telephone lines. Another example of the everyday, which concerns the storage this time, is the alteration of the data read on an optical disk because of scratches or jumps of the reading lens (during a sudden movement).

The error correction codes must therefore enable us to obtain, as far as where possible, all the data read.

The objective of this work is to prove that it's possible to reduce a large number of components in the Chien Search Block by using a new method called factorization method which followed us to conceive another circuit of Chien Search Block [1].With an important number of minimized logic gates.

The modified circuit will be compared to the basic circuit in order to show the difference between the two circuits and the percentage of the reduced power consumption.

II. REED SOLOMON CODE

A Reed-Solomon code [2] is a block code and can be specified as RS (n,k) as shown in Fig. 1. The variable n is the size of the codeword with the unit of symbols, k is the number of data symbols and 2t is the number of parity symbols Each symbol contains s number of bits.

Fig.1. RS code word structure.

- Block length : $n= 2^{m-1}$
- Nounber Of parity check bits $r= n-k \leq m*t$
- Minimum distance $dmin \geq 2t + 1$

II.1 REED-SOLOMON ENCODER:

Achieving the Reed-Solomon RS [3] codes is as follows:
1.Build the body of the Galois GF (q^m)
Error correcting codes operate over a large extent on powerful algebraic structures called finite fields. A finite field is often known as Galois field after Pierre Galois, the French mathematician. A field is one in which addition, subtraction, multiplication and division can be performed on the field elements and thereby obtaining another element within the set itself. A finite field always contains a finite number of elements and it must be a prime power, say q = pr, where p is prime. There exists a field of order q for each prime power q = pr and it is unique. In Galois field GF (q), the elements can take this q different values. We are exploiting the following properties of a finite field:

a. Addition and multiplication operations are defined.
b.The result of addition or multiplication of two elements is always an element in the field.
c. Zero is an element in the field, such that a + 0 = a for any element a in the field.
d. Unity is an element in the field, such that a • 1 = a for any element a in the field.

2. Determine a primitive polynomial using the nth root α in the Galois field GF (q^m)
3. Choose 2t = γ -1 α consecutive power.
4. Build generator polynomial g (x) as the least common multiple LCM of minimal polynomials associated with the power to choose α.

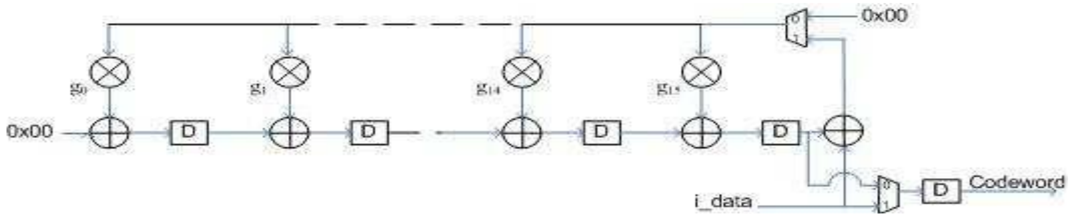
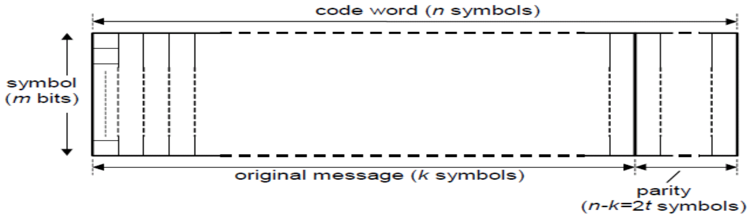


Fig.2 Encoding circuit for RS (n, k) code

II.2 REED SOLOMON DECODING:

Reed-Solomon Decoder[4]consider the incoming message as a polynomial R(x), transmitted message as T(x) and Error introduced as polynomial E(x). i.e.
R(X) = T(x) + E(x)
Now the Decoder problem is to identify the E(x) so that T(x) can be calculated as follows:
T(X) = R(x) + E(x)



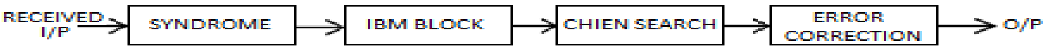


Fig 3: Block Diagram of RS Decoder

The RS decoder normally consists of four modules namely:

- Syndrome Calculator.
- Inversion less Berlekamp Algorithm.
- Chien Search.
- Error Correction.

1. Syndrome Calculator:

The syndrome calculator[5]is the first module of the RS decoder. The input to this module is the corrupted codeword. The equations for the codeword, received bits and the error bits are given as below.

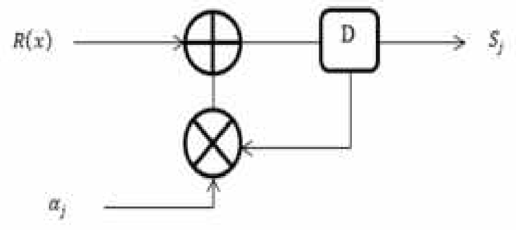


Fig 4.shéma of syndrome bloc

2. Berlekamp’s algorithm:

Berlekamp’s algorithm [6] is a more efficient iterative technique of solving equations that also overcomes the problem of not knowing ν. This done by forming an approximation to the error locator polynomial, starting with A(x) = 1. Then at each stage, an error value is formed by substituting the approximate coefficients into the equations corresponding to that value of ν. The error is then used to refine a correction polynomial, which is then added to improve the approximate A (x). The process ends when the approximate error locator polynomial checks consistently with the remaining equations.

The error locator polynomial

The error locator polynomial A(x) and the error evaluator polynomial Ω(x), which can be represented in the general form shown in (1) and (2) respectively.

i. $A(X) =\prod^{e}_{j=1}(1+X_j x)$

1. (1)

ii. $\Omega(x)= \sum^{e}_{i=1} X_i Y_j \prod^{e}_{j=1}(1+X_j x)$

The error locator polynomial, A(x), has a degree of e < t.

The error evaluator polynomial, Ω(x) has degree at most e-1 to determine the magnitude of e errors. There are different algorithms that have been used to solve the key equation and two common ones are the Euclidean algorithm.

$$A(x) = \prod_{i}^{v}(1 + X_i x)$$

i. $= X1(x + X_1^{-1})X_2(x + X_2^{-1})$…..

With: $X1=\alpha^{e1}$, $X2= \alpha^{e2}$ … then clearly the function value will be zero if $x= \alpha^{-e1}$, $x=\alpha^{-e2}$ …

3. Chien search algorithm:

This algorithm can detect the error position by calculating $\Lambda (\alpha^{-i})$ with $0 \le i \le n-1$, such as Λ (x) is the error locator polynomial, previously calculated with the Euclidean algorithm. For the case of RS (n, k) we must calculate:

$$A(\alpha^{-(n-1)}),\ A\left(\alpha^{-(n-2)}\right)\cdots A(\alpha^{-1}),\ A(\alpha^{-0})$$

If the expression reduces to 0 $\Lambda(\alpha^{-i}) = 0$, then that value of x is a root and identifies the error position else the position does not contain an error.

A. Factorization method:

The factorization method is the method in which we factorize the error locator polynomial as form $\prod^{n}_{i=1}(\alpha X+\beta)$ such that (α, βi) ϵ (GF) Galois Field. And with this method we can conceive another form of the circuit of the Chien Search i.e. we can minimize a large number of the used logic gates in the circuit, and therefore we will have a low power consumption on this circuit [7]. If we take the case of RS (15, 11, t) the error locator polynomial is:

$$A(x) = 14x^2 + 14x + 1$$

It's a polynomial of drgree 2 as type:

$$\begin{aligned}\Lambda(x) &= A_2X^2+A_1X+ A_0\\ &= (AX+B)(AX+C)\end{aligned}$$

The equation (5) can be written as form:

$$\begin{aligned}\Lambda(x) &= (\alpha X+\beta)(\alpha X+\gamma)\\ &= \alpha^2X^2 +\alpha X\gamma+ \alpha X\beta+\beta\gamma\\ &= \alpha^2X^{2+}\alpha(\gamma+\beta)X+\beta\gamma \qquad (6)\end{aligned}$$

Or $A_2 = \alpha^2, A_1 = \alpha(\gamma+\beta)$ and $A_{0=}\ \beta\gamma$

For equation (5) the basic circuit corresponding is represented in figure 5.
The simulation of the basic circuit (equation 5) with Quartus II is represented in figure 8.
For the equation (6) the modified circuit by using the factorization method is represented in figure6.
The simulation of the modified circuit (equation 6) with Quartus II is represented in figure 9.

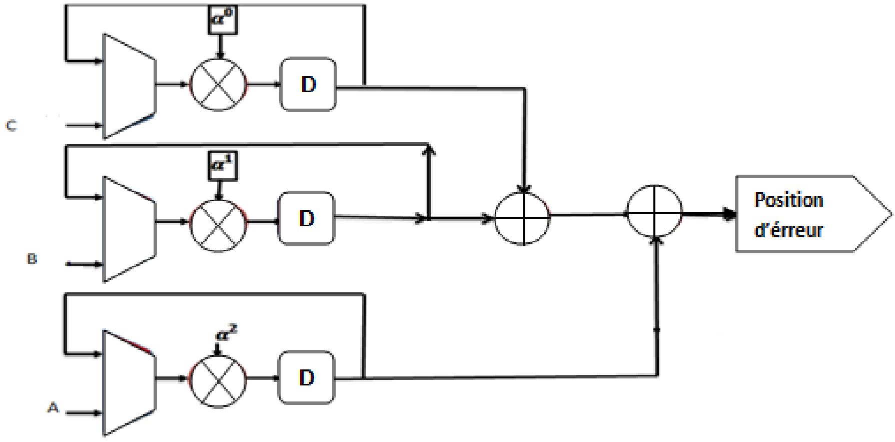


Fig. 5 Basic schema of Chien Search.

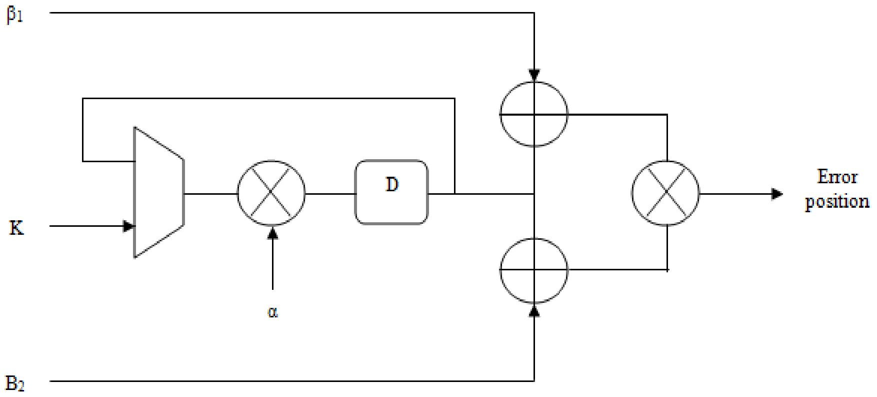


Fig.6 Modified circuit of Chien Search.

For the case of a polynomial of degree 3 we have:

$$\Lambda\ (X) = (\alpha X+\beta)\ (\alpha X+\gamma)\ (\alpha X+\lambda)$$
$$= (\alpha^2 X^2 + \alpha\ (\gamma + \beta)\ X + \beta.\gamma)\ (\alpha\ X+ \lambda)$$

Generally for:

$$\Lambda\ (X) = (\alpha X+\beta)\ (\alpha X+ \gamma)\ \ldots\ (\alpha X+\nu)$$

The corresponding logic circuit is represented in figure

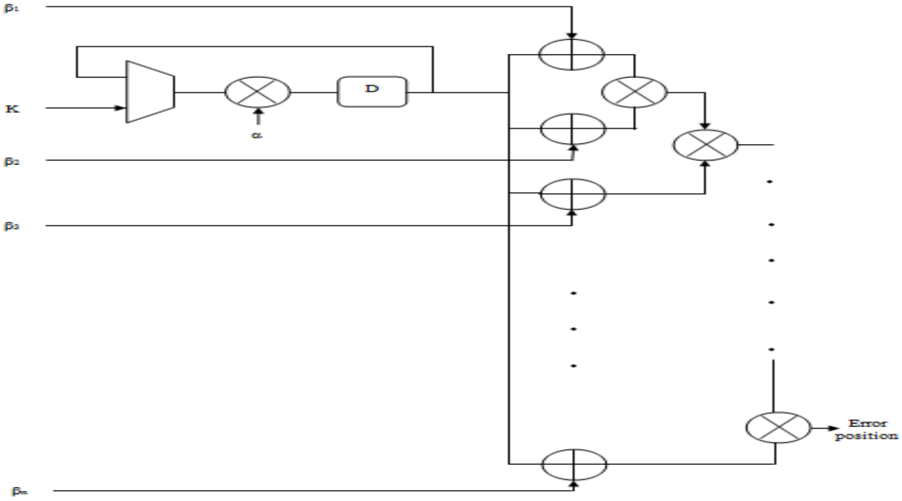


Fig.7. Modified circuit of Chien Search.

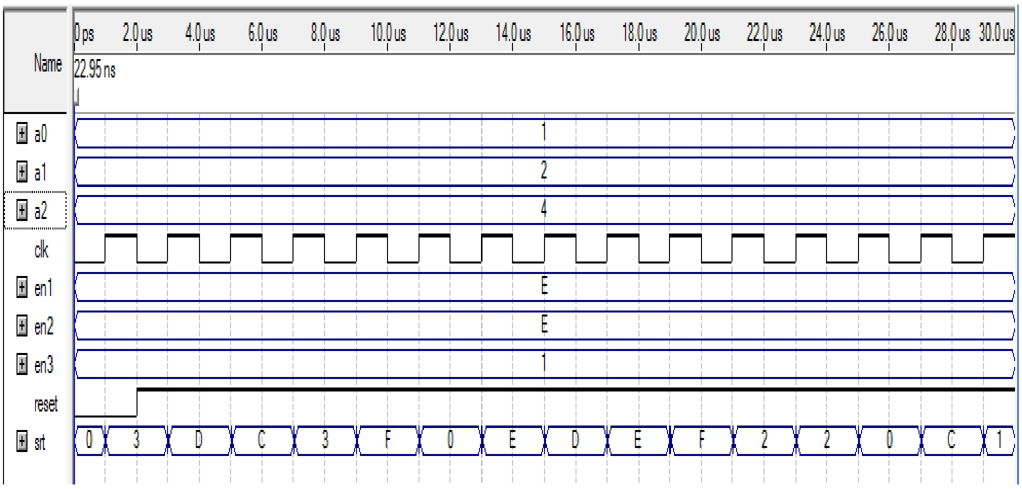


Fig.8. Simulation of the basic circuit (equation 4) with Quartus II.

With a0, a1 et a2 represent respectively α^0, α^1, et α^2 of figure 2, And en1, en2 et en3 represent respectively A, B et C.

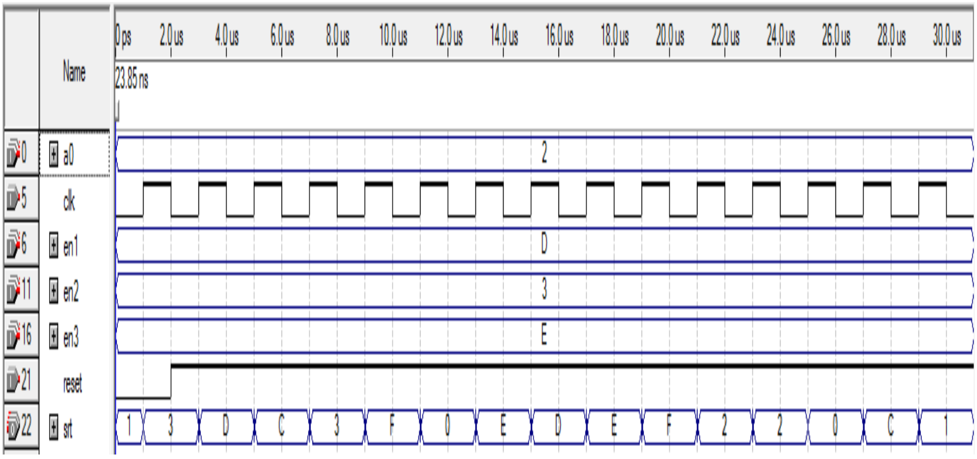


Fig.9. Simulation of the modified circuit (equation 5) with Quartus II.

With a0 represent α of figure 4 and srt represent the error position and en1, en2, en3 represent respectively α, β1, β2

B.Comparison of circuits:

modified circuit but with an important number of minimized logic gates. This minimization can save a percentage of power which can reach 50% compared to the basic circuit.

The table 1, shows the number of the used logic gates by using the basic circuit and the number of used logic gates by using the modified circuit for different error locator polynomials.

Error locator polynomial	Number of logic gates for the basic circuit	Number of logic gates for the modified circuit	Number of minimized logic gates
$A(X) = AX^2 + BX + C$	11	6	5
$A(X) = AX^3 + BX^2 + CX + D$	15	8	7

$A(X) = AX^4 + BX^3 + CX^2 + DX + E$	19	10	9
$\vdots$			
$A(X) = A_nX^n + A_{n-1}X^{n-1} + \cdots + A_1X + A$	$3 + 4n$	$3 + (2n - 1)$	$2n + 1$

Table number of minimized logic gates for different error locator polynomials.

III. CONCLUSION

The modified circuit depends on the degree of error locator polynomial. The more the degree of locator polynomial increases the more the number of minimized logic gates becomes more important and takes as value the double of polynomial degree plus 1. in other words, if the polynomial degree is n, deg (P (X)) = n then the number of minimized logic gates is 2n+1. This minimization reduces the power consumption [8] with a percentage which can reach 50 % compared to the basic circuit [9] and plays a very important role in the standard DVB and in particular the standard DVB-T. Finally the factorization method is a new method which can be considered an added value [10] for the chien search block and mainly Reed-Solomon codes, which reduces a large number of used logic gates.

REFERENCES

[1]. P. Djiknavorian, Codes de Reed-Solomon Etude et simulation, avril 2007.

[2]. BBC Research and Development, Reed-Solomon error correction, British Broadcasting Corporation, 2002.

[3]. Jean-yves chouinard, théorie et pratique des codes correcteurs, janvier 2013

[4]. R. Huynh, G. Ning and Y. Huazhung, A Low Power Error detection in the syndrome calculator Block for Reed-Solomon codes RS: (208,188), J. Tsinghua Science and Technologie, 14(4), 2009, 474-477.

[5]. VJ.Babrekar, SV. Sakhare, Review of FPGA Implementation of Reed-Solomon Encoder- Decoder, International Journal of Computer Applications, 87(8), 2014, 16–19.

[6]. BBC Research and Development, Reed-Solomon Error Correction ,British Broadcasting Corporation, 2002.

[7]. A. El habti, R. Elgouri and L. Hlou, A low power error detection in the chien search block for reed-solomon code, university of science kenitra, 2012.

[8]. J. Allen, Energy efficient adaptive Reed-Solomon decoding System,university of Massachusetts Amherst in partial fulfillment of the requirements for the degree of master of science in electrical and computer engineering,2008.

[9]. P.Beelen, K. Brander, “List decoding of Reed–Solomon codes from a Gr¨obner basis perspective,”J. Journal of symbolic computation, vol. 45, pp. 773-786, January 2008.

[10]. B.Y Bing, E.G. Zeng,” New concatenated soft decoding of Reed-Solomon codes with lower complexities,” The Journal of China Universities of Posts and Telecommunications,vol. 16, pp. 4-7 June 2009.

Elghayyaty Mohamed ‘Minimized Logic Gates Number Of Components In The Chien Search Block For Reed-Solomon (RS)” American Journal of Engineering Research (AJER), vol. 7, no. 2, 2018, pp. 110-116.