© 2014 IJIRT | Volume 1 Issue 7 | ISSN: 2349-6002

R.S. ENCODERS OF LOW POWER DESIGN

R. Anusha[1], D. Vemanachari[2]
[1]*M.Tech, ECE Dept, M.R.C.E, Hyderabad,*
[2]*PhD, Associate Professor and H.O.D, ECE Dept., M.R.C.E. Hyderabad*

***Abstract*— High speed data transmission is the current scenario in networking environment. Cyclic redundancy check (CRC) is essential method for detecting error when the data is transmitted. About the speed of transmitting data, and to synchronize with speed, it is necessary to increase speed of CRC generation. Starting from the serial architecture a recursive formula was used from which parallel design is obtained. But in this paper presents 64 bits parallel CRC architecture based on F matrix with order of generator polynomial is 32. It is hardware efficient and required 50% less cycles to generate CRC with same order of generator polynomial. Reed-Solomon (RS) codes are one of the most widely used block error-correcting codes in modern communication and computer systems. Multiplication is the key computation in RS encoding. Adopting the generator polynomial with symmetric coefficients, the number of multipliers in RS encoders can be reduced by half, and their power consumption may also reduce.**

***Index Terms*— Carry correction, modular adder, parallel prefix, residue number system (RNS), VLSI.**

I. INTRODUCTION

Digital communication system is used to transport an information bearing signal from the source to a user destination via a communication channel. Cyclic redundancy check is commonly used in data communication and other fields such as data storage and data compression, as a essential method for dealing with data errors [6]. Usually, the hardware implementation of CRC computations is based on the linear feedback shift registers (LFSRs), which handle the data in a serial way. the serial calculation of the CRC codes cannot achieve a high throughput. In contrast, parallel CRC calculation can

significantly increase the throughput of CRC computations. Here the throughput of the 32-bit parallel calculation of CRC-32 can achieve several gigabits per second.

The increasing demands for high-density and high performance integrated circuits dictate the Built-In Self Test (BIST) schemes to guarantee high fault coverage, which is expected to be produced by a simple test-pattern generator in an acceptable number of vectors. The BIST involves performing the test-vector generation and the output-response analysis on a chip through the built-in hardware. BIST is a powerful Design For-Testability (DFT) technique for addressing highly complex Very-Large-Scale Integration (VLSI) testing problems. BIST designs include on-chip circuitry to provide test patterns and analyze output responses. Performing tests on the chip greatly reduces the need for complex external equipment. The main motivation for considering power consumption during testing is generally, a circuit consumes much more power in test mode than in normal mode. BIST techniques are mainly employed to improve the circuit's fault coverage, test application time, and test development efforts.

Reed-Solomon (RS) codes are among the most popular error-correcting codes applied in many fields such as digital communication and storage systems. They could detect and correct multiple random symbol errors, particularly well-suited to the situation where errors occur in bursts. RS encoders usually use a linear feedback shift register (LFSR) architecture [1] [2]. Many factors have influence on its encoding power consumption, such as multipliers, corresponding primitive polynomials and generator polynomials.

For a certain RS code which can correct t error symbols, its encoder consists of 2t multiplication so that multipliers can partly determine the power consumption of encoders. Noting that feedback terms are known, the implementation circuit just needs 2t one-input constant multipliers (CM), which have lower circuit complexity, smaller area and shorter critical path than standard two-input multipliers. The primitive polynomial is another crucial factor, whose weight has an immediate relationship with the tuple presentation of each element as well as circuit complexity of its corresponding CM.

Hence to reduce the encoder power consumption, selecting an appropriate one is effective.

A. Reed-Solomon Encoding Algorithm

This paper focuses on an (n, k) RS code whose codeword is a block of n symbols, including k symbols of information and 2t = n-k symbols of redundancy check. It is generated from the k information symbols and t is the maximum number of error corrections. Each symbol is an element of GF(2m) and can be described in m-tuple representation [3]. Considering a k-symbol message (f0, f1, . . . , fi, . . . , fk−1) (fi∈GF(2m), 0 ≤ i <k) as the coefficients of a degree k-1 message polynomial f (x) = f0 + f1x + . . . + fk−1xk−1, the corresponding codeword polynomial with a degree of n-1 can be expressed as c(x) = f(x)g(x) = c0 + c1x + . . . + cn−1xn−1, where the n-symbol codeword (c0, c1, . . . , ci, . . . , cn−1) belongs to GF(2m) and 0 ≤ i < n. RS encoding consists of multiplication of a feedback term with several known items. Given α as the primitive element over GF(2m), the generator polynomial of a primitive t-error corrective RS code with length of 2m – 1 is

$$\begin{aligned} g(x) &= (x+\alpha^{d})(x+\alpha^{d+1})\dots(x+\alpha^{d+2t-1}) \\ &= g_0 + g_1 x + \dots + g_{2t-1}x^{2t-1} + x^{2t} \end{aligned}$$

g(x) has αd, αd+1, . . . , αd+(2t−1) as all its roots and its coefficients (g0, g1, . . . , g2t−1) also belong to GF(2m). The choice of d will not affect the dimension or the minimum distance of the codes.

B. Reed-Solomon Encoder Architecture

The systematic encoding [4] is often accomplished with an LFSR-based circuit. An asymmetric encoder is shown in Fig. 1. Clearly, changing d can obtain different encoding implementation. To reduce the complexity of the encoder, multiplication is implemented by CMs. Especially, when d = 2m−1 − t, the coefficients of the generator polynomial are symmetric and g(x) = 1+g1x+. . .+gtxt+. . .+g1x2t−1+x2t. The corresponding architecture of the symmetric encoder is shown in Fig. 2. The entire encoding process takes n clock cycles. During the first k clock cycles, all the two multiplexors in Fig. 1 select 'a' ports and k symbols are input to the LFSR-based encoder serially with the most significant symbol first.

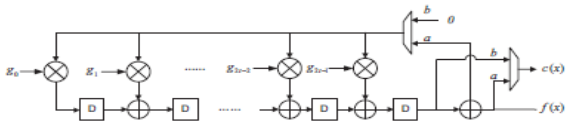
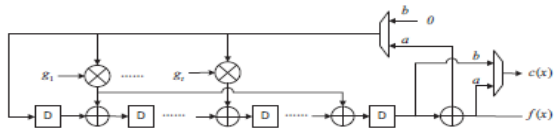


Fig. 1. Asymmetric encoder



Meanwhile, the message is also sent to the output to form the systematic part of the codeword. After k clock cycles, the registers contain n−k symbols of redundancy check. At this time, the multiplexors select 'b' ports and the remainders are shifted out from the registers to form the rest of the codeword. The critical path of the architecture above consists of one XOR gate and one CM. A same process also presents in Fig. 2.

III. ENCODER POWER ANALYSIS

A. Finite Field Multipliers

The key operation in RS encoding is multiplication [5]. In this paper, we research CMs based on the Mastrovito multiplier [6], whose computation processes are clearly described in [7]. The number of gates each CM requires depends on the primitive polynomial used to generate the field and the constant multiplicand.

Each element over the field GF(2m) will be represented by a polynomial of degree m-1. The word-level multiplication operation receives two m-bit input polynomials a(x) = am−1xm−1+am−2xm−2+. . .+a0 and b(x) = bm−1xm−1+ bm−2xm−2 +. . .+b0, where ai, bi ∈ GF(2) and 0 ≤ i < m. The output result is v(x) = a(x)b(x) mod p(x), where p(x) is the primitive polynomial. In the CM case, we consider b(x) the constant multiplicand.

The hardware implementation of a two-input multiplier needs m2 AND and (m−1)2 XOR gates. As for the CM-based RS encoding, m AND and m XOR gates will be removed for each '0' in the m-tuple representation of the constant element b(x), while each '1' results in a reduction of m AND gates. Therefore the circuit complexity of each CM should be determined by both the primitive polynomial and the known item b(x).

B. Primitive Polynomial

Table I shows the effect of primitive polynomials on the CMs over GF(25), GF(28) and GF(210). Each AND gate requires 3/4 the area of an XOR. The area consumptions to be equivalent XOR gate complexities are listed [8]. Obviously, the hardware requirements in α1, α2m−2 ∈ R are much less than the mean area of all the multipliers. What should be noticed is that the CMs with high-weighted p(x) have less means and variances over the whole fields while the low-weighted lead the CMs in R to reduce circuit complexity and power consumption more effectively. That is because higher weights of primitive polynomials tend to increase the complexity of the expression between input and output. Nevertheless, more intermediate computation items have opportunities to be reused so that the circuit

complexity and power consumption decline. The expressions about CMs in R are just simple without many intermediates, so the low-weighted primitive polynomials are better.

C. Generator Polynomial

At the last of Section III-A, we present that the symmetric encoder is usually considered to be the most energy-efficient but there will be other possibilities in asymmetric encoders that lead to even lower power.

Algorithm A: Search for generator polynomials

Input: $g(x) = (x+\alpha^{d})(x+\alpha^{d+1})\dots(x+\alpha^{d+2t-1})$,
$\forall d \in \{0,\ 1,\ 2,\ \dots 2^m-2\},\ l=0,\ v=0,\ S=\varnothing$

Step 1: for $i = 0$ to $2t-1$
begin
for $j = 0$ to 2^m-2
if $(g_i(d_j)$ mod $\alpha^{2^m-1} = \alpha^0$ and $d_j \notin S)$
$v = v+1,\ d_v = d_j;$
end
$S = \{d_1, d_2, \dots, d_v\};$

Step 2: for $\rho = 1$ to v
begin
$g(x) = (x+\alpha^{d_\rho})(x+\alpha^{d_\rho+1})\dots(x+\alpha^{d_\rho+2t-1});$
for $\eta = 0$ to $2t-1$
if $g_\eta \in R\ \ l = l+1;$
d' = $argmax_l(d);$
end

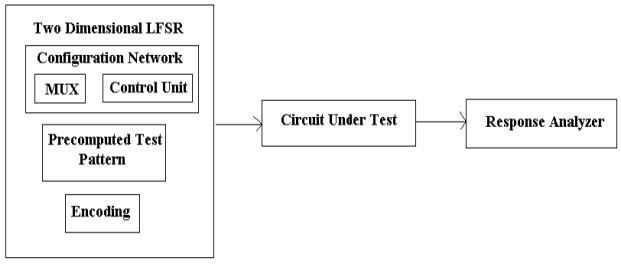
Output: d'

RELATED WORK

Two-Dimensional (2-D) Linear Feedback Shift Registers (LFSRS)

A 2-D LFSR-based test pattern generator is proposed to generate an embedded deterministic sequence of test patterns followed by pseudorandom patterns. The generator mainly consists of four types of function blocks:

• Flip-Flop Array (FFA)
• Configuration Networks (CN)
• Multiplexers (MUXs)
• Control Unit (CU)



Circuit under Test (CUT)

Circuit under test is the circuit which is to be tested to find the faults present in that circuit. Controllability, observability and predictability are the three most important factors that determine the complexity of driving a test for a circuit. A circuit under test fails when its observed behavior is different from its expected behavior.

Output Response Analyzer (ORA)

The Output Response Analyzer (ORA) compacts the output responses of the CUT to the many test patterns produced by the TPG into a single Pass/Fail indication. The output response analyzer is sometimes referred to as an Output Data Compaction (ODC) circuit. The significance of the output response analyzer is that there is no need to compare every output response from the circuit under test with the expected output response external to the device.

Only the final Pass/Fail indication needs to be checked at the end of the BIST sequence in order to determine the fault- free/faulty status of the CUT.

Precomputed test pattern generation

For BIST in general, test patterns are generated on-chip by a TPG and the responses of the CUT are compressed and analyzed by an on chip signature analyzer. There are generally three strategies of test:

(1) Exhaustive Test
(2) Deterministic Test
(3) Pseudorandom Test

Steps to generate precomputed test pattern:-

1) Set F to be the set of all target faults (a set of detectable faults). Set K equal to the number of primary inputs.
2) If F is empty, stop.
3) Generate N random patterns by fixing the inputs that have a weight 0 (1), and randomly specifying the other inputs (N is a predetermined constant).
4) For each random pattern generated, perform fault simulation for every fault f.
5) If f is detected, remove f from F.
6) If no fault was detected by the previously applied N tests, set K = K - 1.
7) Go to Step (2).

Configurable 2-D LFSRs

A 2-D LFSR-based test pattern generator is proposed to generate an embedded deterministic sequence of test patterns followed by pseudorandom patterns. The generator mainly consists of four types of function blocks: - the Flip-Flop Array (FFA), the Configuration Networks (CN), the Multiplexers (MUXs), and the Control Unit (CU). The FFA is an N*M flip-flop array, where is the N number of inputs of a circuit under test (CUT) and M is the number of stages

of the 2-D LFSR. To reduce the hardware, M is usually a small number. Each CN consists of XOR gates and an inverter if necessary. The MUX selects one of the configuration networks to feed the feedback signals to the FFA. The MUX is controlled by the CU. When resetting the generator, the initial states of FFA are set to alternating 1 and 0, in each column of the FFA [9].

IV. CONCLUSION

In this paper, we analyze the low power design of RS encoders. All factors such as multipliers, primitive polynomial and generator polynomial are discussed in details. Simulation results show that in the case of t = 2, there exists g(x) with asymmetric coefficients which makes the encoder power consumption lower than the symmetric encoders. And low weighted primitive polynomials are better. While t > 2, the symmetric encoders have better power performance. In addition, a method to find the proper generator and primitive polynomial quickly is also proposed.

The complexity of the best found basis in each extension field between F2 2 and F2 24 is in fact lower than for the standard bases. Sometimes the best found complexities coincide, but this is the case only for lower dimensions.

REFERENCES

[1] M. Ayinala and K. K. Parhi, High-Speed Parallel Architectures for Linear Feedback Shift Registers, IEEE Trans. Signal Processing, vol. 59, no. 9, pp. 4459-4469,Sept. 2011.

[2] C. Cheng and K. K. Parhi, High Speed VLSI Architecture for General Linear Feedback Shift Register (LFSR), in Proc. Signals, Systems and Computers, 2009, pp. 713 - 717.

[3] S. Lin and D. J. Costello Error Control Coding: Fundamentals and Applications. Pearson-Prentice Hall, 2004.

[4] G. Seroussi, A Systolic Reed-Solomon Encoder, IEEE Trans. Info. Theory, vol. 37, no. 4, pp. 1217-1220, Jul. 1991.

[5] C. K. Koc and T. Acar, Montgomery Multiplication In GF(2k), Designs, Codes And Cryptography, vol. 14, no. 1, pp. 57-69, Apr. 1998.

[6] E. D. Mastrovito, VLSI Designs For Multiplication Over Finite Fields GF(2m), vol. 357, pp. 297-309, 1989.

[7] J. Lv and P. Kalla, Formal Verification Of Galois Field Multipliers Using Computer Algebra Techniques, in Proc. IEEE Intl. VLSI Design (VLSID), 25th, 2012, pp. 388-393.

[8] X. Wu, X. Shen and Z. Zeng, An Improved RS Encoding Algorithm , in Proc. IEEE Consumer Electronics, Communications and Networks, 2nd, 2012, pp. 1648-1652 ..

[9] Campobello, G.; Patane, G.; Russo, M.; "Parallel CRC realization," Computers, IEEE Transactions on , vol.52, no.10, pp. 1312- 1319, Oct.2003

[10] Albertengo, G.; Sisto, R.; , "Parallel CRC generation," Micro,IEEE , vol.10, no.5, pp.63-71,Oct1990

[11] M.D.Shieh et al., "A Systematic Approach for Parallel CRC Computations," Journal of Information Science and Engineering, May 2001.

[12] Braun, F.; Waldvogel, M.; , "Fast incremental CRC updates for IP over ATM networks," High Performance Switching and Routing,2001 IEEE Workshop on , vol., no., pp.48-52, 2001

[13] Weidong Lu and Stephan Wong, "A Fast CRC Update Implementation", IEEE Workshop on High Performance Switching and Routing ,pp. 113-120, Oct. 2003.

[14] S.R. Ruckmani, P. Anbalagan, " High Speed cyclic Redundancy Check for USB" Reasearch Scholar, Department of Electrical Engineering, Coimbatore Institute of Technology, Coimbatore-641014, DSP Journal, Volume 6, Issue 1, September, 2006.

[15] Yan Sun; Min Sik Kim; , "A Pipelined CRC Calculation Using Lookup Tables," Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE , vol., no., pp.1-2, 9-12 Jan. 2010

[16] Sprachmann, M.; , "Automatic generation of parallel CRC circuits," Design & Test of Computers, IEEE , vol.18, no.3, pp.108-114, May 2001.

AUTHOR DETAILS:

First Author: ***R. Anusha*** received B.Tech Degree in Electronics and Communication Engineering from Sridevi Women's Engineering College in the year of 2011. She is currently M.Tech student in Em & VLSI Design from Malla Reddy College of Engineering. And her research interested areas in the field of High-speed low-power DSP technology with VLSI, NoC, Wireless Communications, and Software Radio.

Second Author: ***D. Vemanachari*** working as an Associate Professor and H.O.D ECE Department in Malla Reddy College of Engineering. He has completed his M.Tech and he has 15+ years of teaching experience. His research interested areas are High-speed low-power DSP technology with VLSI, NoC, Wireless Communications, and Software Radio.