ISSN: 0975-3583,0976-2833 VOL12, ISSUE 02, 2021

Enhancing Medical Data Integrity: Transformation of LFSR Circuits for Improved Performance

G. Vishwanath

Vice Principal, Associate Professor and Head, Department of Electronics and Communication Engineering.

Kakatiya Institute of Technology and Science for Women, Manik bhandar, Nizamabad, Telangana, India.

Abstract

Linear Feedback Shift Registers (LFSRs) are integral to various medical applications, particularly in cyclic redundancy check (CRC) operations and BCH encoders. This thesis establishes a mathematical proof demonstrating the feasibility of transforming LFSR circuits into equivalent state space formulations, aiming to enhance their performance in medical data processing. The proposed transformation accelerates processing speed compared to serial architectures, albeit with increased hardware overhead. Applicable across all irreducible polynomials used in medical data integrity verification and encoding, a new formulation is suggested to adapt LFSRs into CRC filter structures. Moreover, a novel high-speed parallel LFSR architecture is introduced, emphasizing its suitability for medical data processing. Leveraging parallel Infinite Impulse Response filter design, pipelining, and retiming algorithms, this architecture surpasses previous designs by incorporating both feedforward and feedback paths. Further improvements involve combined parallel and pipelining techniques to mitigate the fanout effect in extended generator polynomials. The proposed scheme offers universal applicability to any generator polynomial, providing comparable critical path performance to previous designs at a reduced hardware cost.

Keywords: Linear Feedback Shift Register, Infinite Impulse Response, cyclic redundancy check, BCH encoders.

1. Introduction

Communication standards continue to be defined that push the bar higher for throughput. For example, 10 Gbps IEEE 802.3ak was standardized in 2003, and recently 100 Gbps IEEE 802.3ba is standardized in 2010. In order to support these high throughput requirements at a reasonable frequency, parallel architectures are required. At the same time, the power consumption and hardware overhead should be kept to a minimum. The research in this thesis is directed towards designing high throughput architectures for two key components of the modern communication standards, CRC/BCH encoders and Fast Fourier Transform (FFT). Cyclic Redundancy Check (CRC) is widely used in data communications and storage devices as an efficient way to detect transmission errors. Examples of digital communication standards that employ CRC include Asynchronous Transfer Mode (ATM), Ethernet (IEEE 802.3), WiFi (IEEE 802.11) and WiMAX (802.16). The Bose-ChaudhuriHochquenghem (BCH) codes are one of the most powerful algebraic codes and are extensively used in modern communication systems. Compared to Reed-Solomon codes, BCH codes can achieve around additional 0.6dB coding gain over the additive white Gaussian noise (AWGN) channel with similar rate and codeword length. Many applications of BCH codes such as long-haul optical communication systems used in International Telecommunication

ISSN: 0975-3583,0976-2833 VOL12, ISSUE 02, 2021

Union-Telecommunication Standardization sector (ITU-T) G.975, magnetic recording systems, solid-state storage devices and digital communications require high throughput as well as large error correcting capability. Hence, BCH codes are of great interest for their efficient and high speed hardware encoding and decoding 1 2 implementation. The BCH encoders and CRC operations are conventionally implemented by a linear feedback shift register (LFSR) architecture. While such an architecture is simple and can run at high frequency, it suffers from serial-in and serial-out limitation. In optical communication systems, where throughput over 1 Gbps is usually desired, the clock frequency of such LFSR based encoders cannot keep up with data transmission rate and thus parallel processing must be employed. Doubling the data width, i.e two parallel architecture doesn't double the throughput, the worst case timing path becomes slower. Since the parallel architectures contain feedback loops, pipelining cannot be applied to reduce the critical path. Another issue with the parallel architectures is hardware complexity.

2 Literature survey

In order to meet the increasing demand on processing capabilities, much research has been carried out on parallel architectures of LFSR for CRC and BCH encoders. In [5], first serial to parallel transformation of linear feedback shift register was described and was first applied to CRC computation in [6]. Several other approaches have been 6 recently presented to parallelize LFSR computations [7], [8], [9], [10].

A novel parallel CRC architecture based on state space representation is proposed in the literature. The main advantage of this architecture is that the complexity is shifted out of the feedback loop. The full speedup can be achieved by pipelining the feedforward paths. A state space transformation has been proposed to reduce complexity but the existence of such a transformation was not proved and whether such a transformation is unique has been unknown so far. In this thesis, we present a mathematical proof to show that such a transformation exists for all CRC and BCH generator polynomials. We also show that this transformation is non-unique. In fact, we show the existence of infinite such transformations and how these can be derived. We then propose novel schemes based on pipelining, retiming and look ahead computations to reduce the critical path in the parallel architectures based on parallel and pipelined CRC filter design.

3 Basic Linear Feedback Shift Registers

CRC computations and BCH encoders are implemented by using Linear Feedback Shift Registers (LFSR)[1], [2], [3]. A sequential LFSR circuit cannot meet the speed requirement when high speed data transmission is required. Because of this limitation, parallel architectures must be employed in high speed applications such as optical communication systems where throughput of several gigabits/sec is required. LFSRs are also used in conventional Design for Test (DFT) and Built in Self Test (BIST) [4]. LFSRs are used to carry out response compression in BIST, while for the DFT, it is a source of pseudorandom binary test sequences. A basic LFSR architecture for Kth order generating polynomial in GF(2) is shown in Fig. 2.1. K denotes the length of the LFSR, i.e., the number of delay elements and g0, g1, g2, ..., gK represent the coefficients of the characteristic polynomial. The characteristic polynomial of this LFSR is

$g(x) = g0 + g1x + g2x\ 2 + ... + gKx\ K$

ISSN: 0975-3583,0976-2833 VOL12, ISSUE 02, 2021

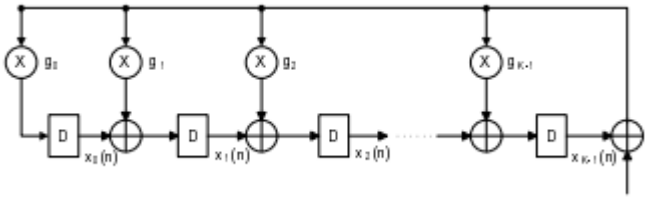

Figure 1: Basic LFSR architecture

where g0, g1, g2, ..., gK ∈ GF(2). Usually, gK = g0 = 1. In GF(2), multiplier elements are either open circuits or short circuits i.e., gi = 1 implies that a connection exists. On the other hand gi = 0 implies that no connection exists and the corresponding XOR gate can be replaced by a direct connection from input to output. Let u(x), for x = 0, 1, ...N − 1, u(x) ∈ GF(2), 0 ≤ n ≤ N − 1 be input sequence of length N. Both CRC computation and BCH encoding involve the division of the polynomial u(x)x K by g(x) to obtain the remainder, Rem(u(x)x K)g(x) . During the first N clock cycles, the N-bit message is input to the LFSR with most significant bit (MSB) first. At the same time, the message bits are also sent to the output to form the BCH encoded codeword. After N clock cycles, the feedback is reset to zero and the K registers contain the coefficients of Rem(u(x)x K)g(x) . In BCH encoding, the remaining bits are then shifted out bit by bit to form the remaining systematic codeword bits. The throughput of the system is limited by the propagation delay around the feedback loop, which consists of two XOR gates. We can increase the throughput by modifying the system to process some number of bits in parallel.

4.proposed method

4.1 State Space Representation of LFSR

A parallel LFSR architecture based on state space computation has been proposed in [13]. The LFSR shown in Fig. 1 can be described by the equation x(n + 1) = Ax(n) + bu(n); n >= 0

with the initial state x(0) = xo. The K-dimensional state vector x(n) is given by x(n) = [x0(n) x1(n)...xK−1(n)]T and A is the K × K matrix given by

$$\mathbf{A} = \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & g_0 \\ 1 & 0 & 0 & \dots & 0 & g_1 \\ 0 & 1 & 0 & \dots & 0 & g_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & g_{K-1} \end{bmatrix}$$

The K × 1 matrix b is b = [g0 g1...gK−1] T .

The output of the system is the remainder of the polynomial division that it computes, which is the state vector itself. We call the output vector y(n) and add the output equation y(n) = Cx(n) to the state equation in (2.1), with C equal to the K × K identity matrix. The coefficients of the generator polynomial g(x) appear in the righthand column of the matrix A. Note that, this is the companion matrix of polynomial g(x) and g(x) is the characteristic polynomial of this matrix. The initial state xo depends on the specific definition of the CRC for a given application.

4.2 State Space Transformation

ISSN: 0975-3583,0976-2833 VOL12, ISSUE 02, 2021

A linear transformation has been proposed [13] to reduce the complexity in the feedback loop. The state space equation of L-parallel system with an explicit output equation is described as

$x(mL + L) = ALx(mL) + BLuL(mL); y(mL) = CLx(mL)$

where CL = I, the K × K identity matrix. The output vector y(mL) is equal to the state vector which has the remainder at m = N/L. Consider the linear transformation of the state vector x(mL) through a constant non-singular matrix T, i.e., x(mL) = Txt(mL)

Given T and its inverse, we can express the state space equation (2.5) in terms of the state vector xt(mL), as follows: $xt(mL + L) = ALtxt(mL) + BLtuL(mL); y(mL) = CLtxt(mL)$

where ALt = T −1ALT; BLt = T −1BL; CLt = T

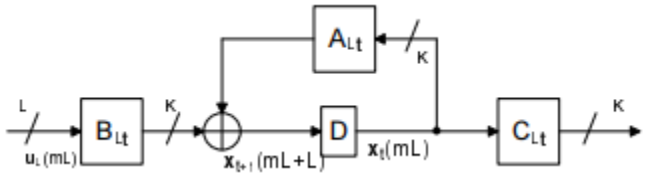

Figure 2: Modified LFSR Architecture using state space transformation

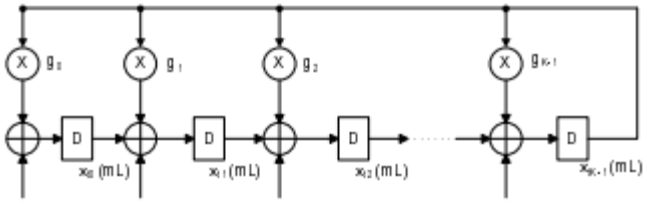

Figure 3: Modified feedback loop of Fig. 2

and T is the transformation matrix. The parallel LFSR architecture after the transformation is shown in Fig. 2 and the modified feedback loop in Fig. 3. We can observe from the figure that if ALt is a companion matrix, then the complexity of the feedback loop will be same as that of the original LFSR. If there exists a T such that ALt is a companion matrix, then the complexity in the feedback loop comes down. It is evident that (2.6) represents a similarity transformation and we can state that there exists a T such that ALt is a companion matrix if and only if AL is similar to companion matrix. The following theorem proves that AL is similar to a companion matrix provided the generator polynomial is irreducible. The latter condition is met for all CRC and BCH codes.

5. Simulation Results

ISSN: 0975-3583,0976-2833 VOL12, ISSUE 02, 2021

Device Utilization Summary (estimated values)			[-]
Logic Utilization	**Used**	**Available**	**Utilization**
Number of Slices	7	4656	0%
Number of Slice Flip Flops	12	9312	0%
Number of 4 input LUTs	12	9312	0%
Number of bonded IOBs	26	232	11%
Number of GCLKs	1	24	4%

fig 4 Design Summary

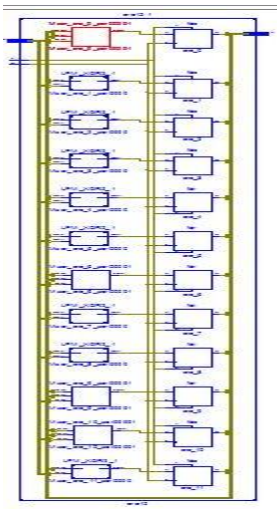

Fig 5 RTL SCHEMATIC

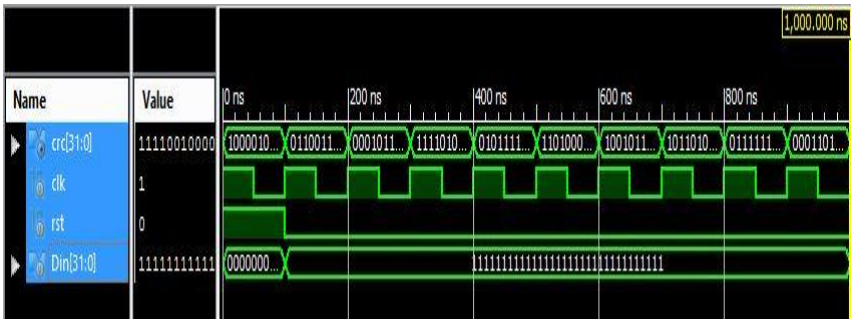

Fig 6 LFSR Based CRC-32

ISSN: 0975-3583,0976-2833 VOL12, ISSUE 02, 2021

```
=========================================================================
Timing constraint: Default OFFSET OUT AFTER for Clock 'clk'
  Total number of paths / destination ports: 12 / 12
-------------------------------------------------------------------------
Offset:              4.252ns (Levels of Logic = 1)
  Source:            crc_0 (FF)
  Destination:       crc<0> (PAD)
  Source Clock:      clk rising

  Data Path: crc_0 to crc<0>
                               Gate     Net
    Cell:in->out      fanout   Delay   Delay  Logical Name (Net Name)
    ----------------------------------------  ------------
     FDS:C->Q              6   0.514   0.569  crc_0 (crc_0)
     OBUF:I->O                 3.169          crc_0_OBUF (crc<0>)
    ----------------------------------------
    Total                      4.252ns (3.683ns logic, 0.569ns route)
                                       (86.6% logic, 13.4% route)

-------------------------------------------------------------------------
```

Fig 7 Time delay

Conclusion

This paper has presented a complete mathematical proof to show that a transformation exists in state space to reduce the complexity of the parallel LFSR feedback loop. This leads to a novel method for high speed parallel implementation of linear feedback shift registers which is based on parallel CRC filter design. Our design can reduce the critical path without increasing the hardware cost at the same time. The design is applicable to any type of LFSR architecture. Further we show that using combined pipelining and parallel processing techniques of CRC filtering, critical path in the feedback part of the design can be reduced. The large fan-out effect problem can also be minimized with some hardware overhead by retiming around those particular nodes.

References

[1] T. V. Ramabadran and S.S. Gaitonde, ”A Tutorial on CRC Computations,” IEEE Micro., Aug. 1988.

[2] R. E. Blahut, Theory and Practice of Error Control Codes. Reading, MA: AddisonWesley, 1984

[3] W. W. Peterson and D. T. Brown, ”Cyclic codes for errot detection”, Proc. IRE, vol.49, pp. 228-235, Jan.1961

[4] N. Oh, R. Kapur, T. W. Williams, ”Fast seed computation for reseeding shift register in test pattern compression,” IEEE ICCAD, 2002, pp. 76-81.

[5] M. Y. Hsiao and K. Y. Sih, ”Serial-to-parallel transformation of linear feedback shift register circuits”, IEEE Trans. Electronic Computers, vol. EC-13, pp. 738- 740, Dec. 1964