ESP-IJCEET
ESP International Journal of Communication Engineering & Electronics Technology
ISSN: 2583-9217 / Volume 1 Issue 3 October 2023 / Page No: 1-6
Paper Id: IJCEET-V1I3P101 / Doi: 10.56472/25839217/ IJCEET-V1I3P101

Original Article

Efficient Majority Voting in Digital Hardware using Geffe Generator

G. Prammasakthi Priya[1], A. SamsuNighar[2]

[1,2]Grace College of Engineering, Tamilnadu, India

Received Date: 02 September 2023 Revised Date: 15 September 2023 Accepted Date: 01 October 2023

Abstract: *Linear-feedback Shift Registers (LFSRs) are pivotal components in digital circuitry, characterized by their ability to generate sequences based on a linear function of their previous states. This paper delves into the fundamental principles, applications, and advancements in LFSR technology.*

LFSRs find extensive use in creating pseudo-random sequences, which are crucial in various domains such as cryptography, communication, and probabilistic algorithms. Understanding the mathematical basis of LFSRs, their feedback polynomials, and tap configurations is essential for designing effective pseudo-random sequence generators. In the context of Built-In Self-Test (BIST) for digital circuits, LFSRs are key to optimizing test pattern generation. Innovations in segmentation techniques and the integration of LFSRs into BIST architectures enhance the efficiency and accuracy of testing procedures. Moreover, this paper explores the role of LFSRs in data compression. By investigating techniques such as Huffman coding and complementary coding, we demonstrate how LFSRs contribute to efficient compression schemes, reducing hardware overhead while maintaining data integrity.

Overall, this research sheds light on the multifaceted applications of LFSRs, from generating pseudo-random sequences to improving digital circuit testing and data compression. By harnessing the power of LFSRs, we advance technology in diverse fields.

Keywords: *Digital Hardware, Geffe, Generator, BIST, LFSR.*

I. INTRODUCTION

In the realm of digital electronics, where data manipulation and secure communication are paramount, the concept of Linear-feedback Shift Registers (LFSRs) holds a significant position. LFSRs are sequential logic circuits capable of generating sequences of binary bits based on a linear function of their previous states. This seemingly simple yet versatile technology finds applications in a wide array of fields, from cryptography to digital circuit testing and data compression.

The fundamental principle underlying LFSRs involves feedback, where the current state of the register influences the generation of subsequent bits. As these bits are deterministic and entirely determined by their previous states, LFSRs are referred to as pseudo-random sequence generators. This deterministic yet unpredictable behavior renders LFSRs indispensable in various critical domains.

This paper aims to delve into the core concepts, practical applications, and recent advancements in LFSR technology. We will explore the mathematical foundations, feedback polynomials, and tap configurations that define LFSRs. Moreover, we will discuss how LFSRs are leveraged in Built-In Self-Test (BIST) architectures to optimize test pattern generation, ensuring the reliability of digital circuits.

Additionally, we will investigate the role of LFSRs in data compression techniques, such as Huffman coding and complementary coding. These methods enable efficient compression while reducing hardware overhead, making LFSRs an essential component in modern data processing and transmission.

In essence, this exploration of LFSRs underscores their pivotal role in the digital age. They contribute to secure communication, enhance digital circuit testing, and facilitate efficient data compression. As we journey through the intricacies and applications of LFSRs, we gain a deeper appreciation for their significance in advancing technology across diverse fields.

II. LITERATURE SURVEY

- Biplab et al. present a novel on-chip Test Pattern Generator (TPG) designed to generate pseudorandom test patterns without encountering prohibited pattern sets (PPS). This innovative TPG ensures high-quality pseudorandom test patterns while maintaining fault coverage comparable to conventional maximal length linear feedback shift register (LFSR) or cellular automaton (CA)-based TPGs.

- Farimah Farahmandi et al. make significant contributions by proposing an automated approach for generating directed tests, guaranteeing bug activation. They also introduce an automatic bug-fixing technique that leverages the remainder terms' patterns and region analysis to detect and rectify errors.

- Bijan Alizadeh et al. propose a method to correct multiple design bugs in gate-level circuits. Their incremental satisfiability-based mechanism reduces correction time and avoids reintroducing old bugs after fixing new ones.

- Cesar et al. introduce a novel approach that harnesses conflict analysis to reuse functional flip-flops as control point drivers. This method achieves impressive test compression results for both stuck-at and transition patterns in industrial designs.

- Vasileios et al. propose an approximate hybrid high radix encoding for signed multiplications. This technique combines accurate radix-4 encoding for significant bits with approximate higher radix encoding for less significant bits, offering configurable energy-accuracy tradeoffs.

- Abou-Auf et al. develop a novel cell-level fault model for addressing delay failures. They introduce a methodology for identifying worst-case test vectors for flash-based FPGA devices subjected to total-ionizing dose, based on the newly developed fault model.

- Manjari Pradhan et al. present a technique for selecting powerful Design for Test (DTS) patterns during manufacturing tests to identify the root causes of observed errors effectively.

- Grzegorz Mrugalski et al. introduce Star-EDT, a deterministic test compression scheme that seamlessly integrates with EDT-based compression. It exploits clusters of test vectors to detect random-resistant faults efficiently, achieving high compression ratios.

- Andreas et al. propose an automatic Test Pattern Generation (ATPG) framework for generating functional test sequences. They extend this framework with a validity checker module (VCM) to specify constraints for the generated sequences.

- Pomeranz describes a procedure to balance fault detection in test sets, improving their quality by redistributing tests and constructing new ones to detect additional faults effectively.

- Bibhas et al. propose an online transparent test technique for detecting latent hard faults in routers' input/output buffers during field operation of NoCs. This technique prevents fault accumulation by periodically repeating tests.

- Abinaya et al. present a non-intrusive Built-In Self-Test (BIST) system for testing FPGAs, consisting of software and hardware components connected via communication channels.

- Tanveer et al. focus on designing and implementing a 64-bit Fibonacci test pattern generator for IC testing, capable of generating lengthy test patterns for ISCAS benchmark circuits.

- Jaynarayan et al. address scan chain and test pattern reordering, proposing a graph-theoretical framework and approximation algorithms for optimizing scan shift time.

- Darshit Vaghani et al. propose secure scan architecture to protect AES cryptochips against scan-based attacks. This architecture ensures security without compromising test, diagnose, and debug capabilities.

- These diverse research contributions highlight the ongoing advancements in test pattern generation, fault detection, and correction techniques, offering innovative solutions to enhance the reliability and security of integrated circuits and digital systems.

III. PROPOSED SYSTEM

In the realm of digital circuitry and computational algorithms, the Linear-feedback Shift Register (LFSR) stands as a fundamental and versatile building block. An LFSR is a shift register whose input bit is determined by a linear function of its previous state, most commonly implemented through exclusive-OR (XOR) operations. This simple yet powerful concept finds extensive use in various applications, from generating pseudo-random sequences to cryptography and VLSI testing.

At its core, an LFSR operates based on an initial value known as the seed. The deterministic nature of the LFSR ensures that the sequence of values it generates is entirely determined by its current or previous state. However, due to its finite number of possible states, it eventually enters a repeating cycle. Remarkably, by carefully selecting the feedback function, an LFSR can produce a seemingly random and extended sequence with a very long cycle.

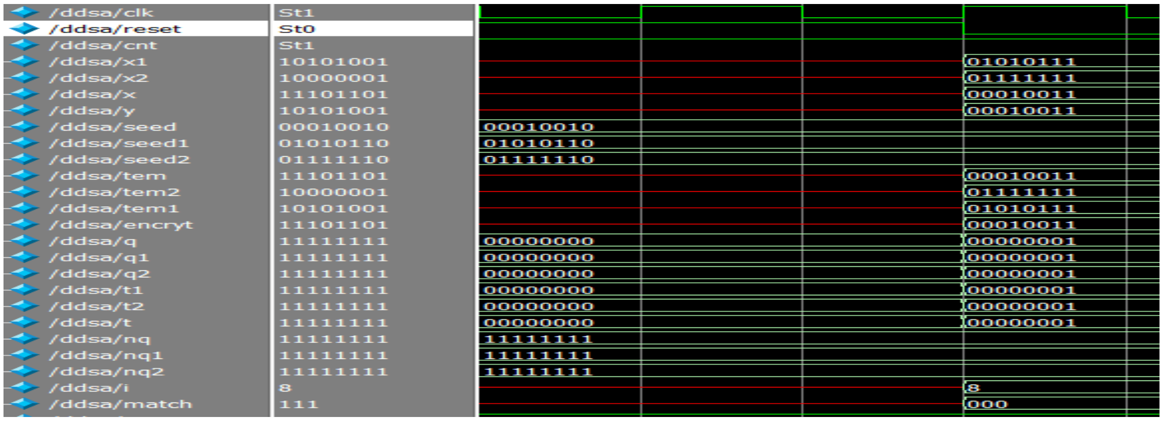
The architecture of an LFSR is defined by its feedback polynomial, expressed in finite field arithmetic as a polynomial mod 2. This polynomial, often referred to as the feedback polynomial or reciprocal characteristic polynomial, consists of coefficients represented as 1s or 0s. The arrangement of taps for feedback, a crucial aspect of LFSR design, is defined by the positions of these coefficients. These taps are essential for creating the linear function that determines the next state of the register.

One powerful application of LFSRs is in the creation of pseudo-random sequences, such as those produced by Geffe generators. Geffe generators employ multiple Linear-feedback Shift Registers, often LFSRs described by primitive polynomials, and a multiplexer to create non-linear forward transformations. These sequences have extensive cycle periods, making them valuable for various applications, including diagnosing faults in combinational and sequential circuits.

Random Number Generators (RNGs) play a pivotal role in diverse fields, including cryptography, communication, and probabilistic algorithms. The goal of an RNG is to produce binary numbers that are statistically independent, uniformly distributed, and unpredictable. To evaluate RNG randomness, seed encryption techniques are often employed to assess their performance. Additionally, in the context of Built-In Self-Test (BIST) for digital circuits, LFSRs play a crucial role in scan-based testing. Innovative approaches utilize LFSRs effectively to achieve maximum cycle lengths and efficient segmentation for test pattern generation.

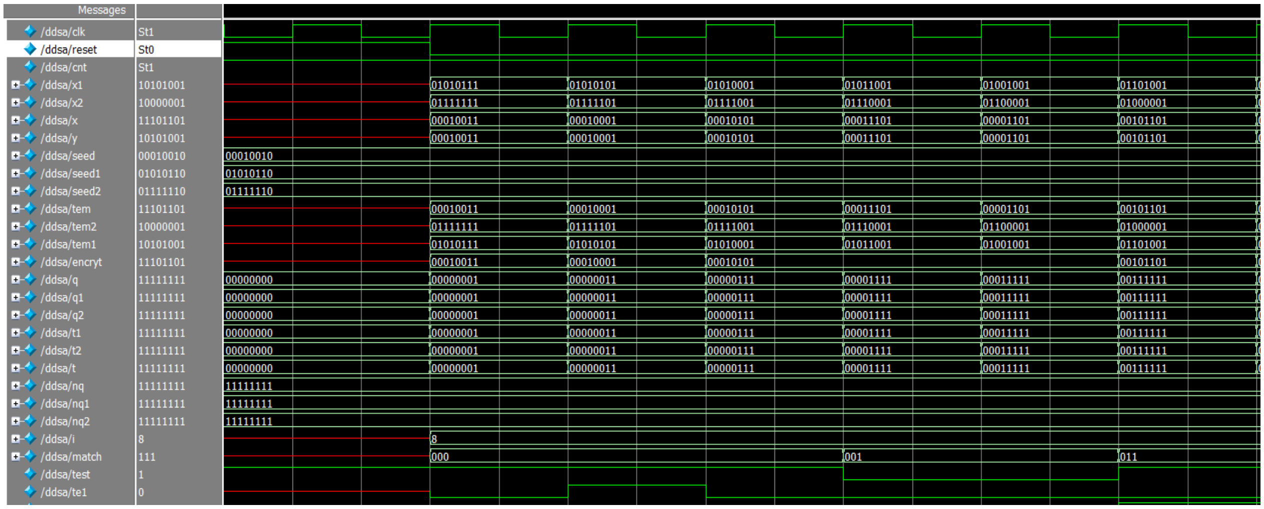
This research explores the foundational concepts of Linear-feedback Shift Registers, delving into their mathematical underpinnings, practical applications, and relevance in modern technology. We investigate their role in generating pseudo-random sequences, optimizing test pattern generation, and enhancing data compression techniques. By comprehensively understanding and harnessing the capabilities of LFSRs, we contribute to the advancement of digital circuit design, cryptography, and data compression methods.

IV. SIMULATION RESULTS



/ddsa/clk	St1
/ddsa/reset	St0
/ddsa/cnt	St1
/ddsa/x1	10101001
/ddsa/x2	10000001
/ddsa/x	11101101
/ddsa/y	10101001
/ddsa/seed	00010010
/ddsa/seed1	01010110
/ddsa/seed2	01111110
/ddsa/tem	11101101
/ddsa/tem2	10000001
/ddsa/tem1	10101001
/ddsa/encryt	11101101
/ddsa/q	11111111
/ddsa/q1	11111111
/ddsa/q2	11111111
/ddsa/t1	11111111
/ddsa/t2	11111111
/ddsa/t	11111111
/ddsa/nq	11111111
/ddsa/nq1	11111111
/ddsa/nq2	11111111
/ddsa/i	8
/ddsa/match	111

Figure 1: Simulation Results

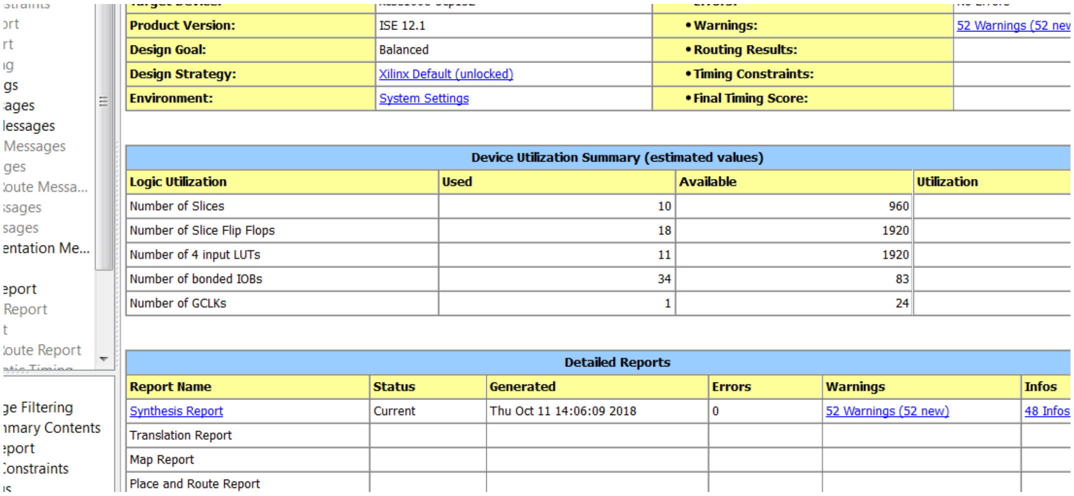


Messages	
/ddsa/clk	St1
/ddsa/reset	St0
/ddsa/cnt	St1
/ddsa/x1	10101001
/ddsa/x2	10000001
/ddsa/x	11101101
/ddsa/y	10101001
/ddsa/seed	00010010
/ddsa/seed1	01010110
/ddsa/seed2	01111110
/ddsa/tem	11101101
/ddsa/tem2	10000001
/ddsa/tem1	10101001
/ddsa/encryt	11101101
/ddsa/q	11111111
/ddsa/q1	11111111
/ddsa/q2	11111111
/ddsa/t1	11111111
/ddsa/t2	11111111
/ddsa/t	11111111
/ddsa/nq	11111111
/ddsa/nq1	11111111
/ddsa/nq2	11111111
/ddsa/i	8
/ddsa/match	111
/ddsa/test	1
/ddsa/te1	0

Figure 2: Simulation Results

V. SYNTHESIS REPORT

The proposed has been simulated and the synthesis report can be obtained by using XILINX. The various parameters used for computing existing and proposed systems are given in the table 1.



Product Version:	ISE 12.1	• Warnings:	52 Warnings (52 new
Design Goal:	Balanced	• Routing Results:	
Design Strategy:	Xilinx Default (unlocked)	• Timing Constraints:	
Environment:	System Settings	• Final Timing Score:	

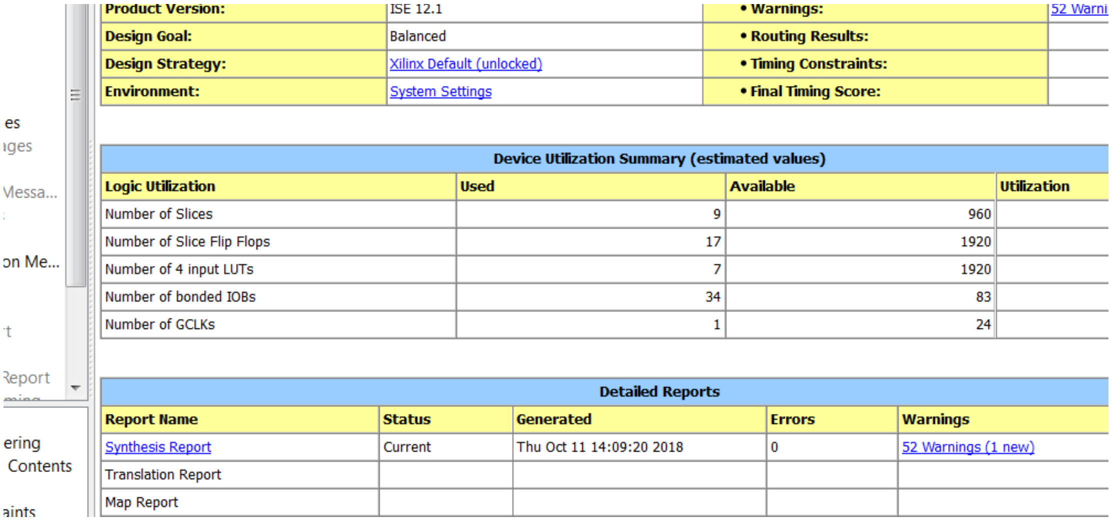
Device Utilization Summary (estimated values)

Logic Utilization	Used	Available	Utilization
Number of Slices	10	960	
Number of Slice Flip Flops	18	1920	
Number of 4 input LUTs	11	1920	
Number of bonded IOBs	34	83	
Number of GCLKs	1	24	

Detailed Reports

Report Name	Status	Generated	Errors	Warnings	Infos
Synthesis Report	Current	Thu Oct 11 14:06:09 2018	0	52 Warnings (52 new)	48 Infos
Translation Report					
Map Report					
Place and Route Report					

Figure 3: Synthesis of Existing



Product Version:	ISE 12.1	**• Warnings:**	52 Warni
Design Goal:	Balanced	**• Routing Results:**	
Design Strategy:	Xilinx Default (unlocked)	**• Timing Constraints:**	
Environment:	System Settings	**• Final Timing Score:**	

Device Utilization Summary (estimated values)

Logic Utilization	Used	Available	Utilization
Number of Slices	9	960	
Number of Slice Flip Flops	17	1920	
Number of 4 input LUTs	7	1920	
Number of bonded IOBs	34	83	
Number of GCLKs	1	24	

Detailed Reports

Report Name	Status	Generated	Errors	Warnings
Synthesis Report	Current	Thu Oct 11 14:09:20 2018	0	52 Warnings (1 new)
Translation Report				
Map Report				

Figure 4: Synthesis of Proposed

Table 1: Comparison Table

S,no	Parameter	Existing	Proposed
1	slices	10	9
2	Slices FF	18	17
3	LUT	11	7

The Figure given below is shown that there is a considerable reduction in time and area based on the implementation results which have been done by using XILINX. The proposed algorithm significantly reduces area consumption when compared to the existing system.

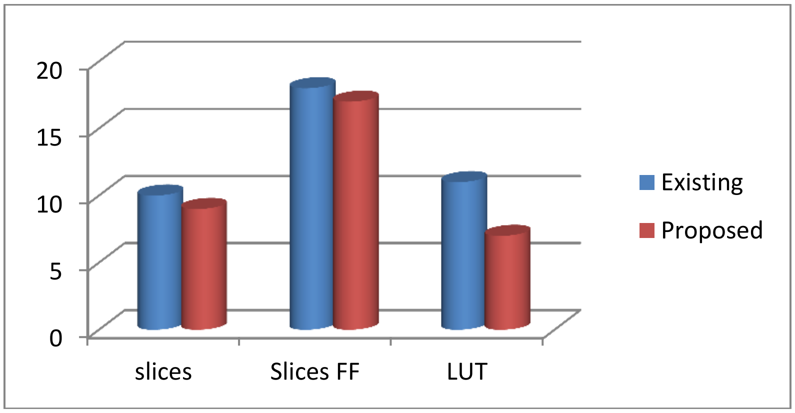


Figure 5: Performance Analysis

IV. CONCLUSION

In conclusion, Linear-feedback Shift Registers (LFSRs) stand as fundamental tools in the realm of digital technology, offering versatility and wide-ranging applications. This paper has provided insights into the core principles and practical applications of LFSRs.

The significance of LFSRs in generating pseudo-random sequences for cryptography, communication, and probabilistic algorithms cannot be overstated. Their deterministic yet seemingly random output makes them invaluable in these domains.

In the context of Built-In Self-Test (BIST) for digital circuits, LFSRs play a vital role in optimizing test pattern generation. The innovative techniques discussed in this paper enhance the efficiency of testing procedures, ensuring the reliability of digital systems.

Furthermore, LFSRs contribute to data compression techniques, with Huffman coding and complementary coding being notable examples. These approaches reduce hardware overhead while maintaining data integrity, making them essential in various applications.

As technology continues to advance, the foundational concepts and practical applications of LFSRs remain relevant. Their role in generating pseudo-random sequences, optimizing testing procedures, and improving data compression methods underscores their importance in the digital age. By harnessing the capabilities of LFSRs, we pave the way for further innovations and advancements in digital technology.

V. REFERENCES

[1] M. Abramovici, M. A. Breuer, and A. D. Friedman, Digital System Testing and Testable Design, IEEE CS Press, New York, 1990.

[2] F. Berglez, D. Bryan, and K. Kozminski, Combinational Profiles of Sequential Benchmark Circuits, Proc. IEEE Int. Symposium on Circuits and System, pp. 1929-1934, 1989.

[3] D. Densmore, “Built-In-Self Test (BIST) implementations an overview of design tradeoffs”, Technical paper, University of Michigan, 2001. [Online]Available: http://www.cs.berkeley.edu/~densmore/documents/BIST.pdfI.

[4] P. R. Geffe, “How to protect data with ciphers that are really hard to break”, Electronics, Vol 46, pp. 99-101, 1973.

[5] P. Girard, “Survey of low-power testing of VLSI circuits”, IEEE Design & Test of Computers, Vol 19, pp. 80 – 90, May-June 2002.

[6] G. Marven, Entropy Based Evaluation of Binary Sequences Produced by ALFSRs, M. Sc. Thesis, Department of Computer Science, University of Victoria, 1994.

[7] M. Puczko and V.N Yarmolik, “Designing cryptographic key generators with low power consumption”, Electronic Design, Test and Applications, 2006. DELTA 2006. Third IEEE International Workshop , pp. 418 – 421, January 2006.

[8] J. Zhong and J. C. Muzio, “A comparison of generators for testing sequential circuits using BIST”, IEEE International Workshop on Logic & Synthesis, pp. 231-235, May 2003.

[9] Livinka S, Divya Dharshini R, 2023. "Smart Traffic Management System Using IoT" ESP Journal of Engineering & Technology Advancements 3(2): 1-7.

[10] J. Zhong and J. C. Muzio, “An investigation of non-linear machines as PRPGs in BIST”, International Conference on VLSI, June 2004.

[11] Bala Murugan P, Kaliammal N, Selvi C, 2022. "Qca Design of Approximate Adder" ESP Journal of Engineering & Technology Advancements 2(3): 5-8.

[12] K. Zeng, C. Yang, D. Wei and T. R. R. Rao, “Pseudoramdom bit generators in stream-cipher cryptography”, IEEE Computer Society, Vol 24, pp. 8-17, February 1991.