A Reversible LFSR Pseudo-Random Sequences Generator

J. Hu
Major Laboratories of integrated circuits
College of Electronic Engineering
Heilongjiang University
Harbin, China

***Abstract*—On the base of reversible sequential circuits, this paper studies the Built-in self-test vector generation method, analyzes the method of LFSRs that generate pseudo-random sequences. Using reversible D Flip-Flops, we build a LFSR pseudo-random sequences generator to realize Built-in Self Test for reversible circuits. It can achieve the maximum length pseudo-random sequence.**

Keywords-reversible circuits; DFT; LFSR

I. INTRODUCTION

With the development of science and technology, many testable design methods have been widely studied and applied to improve the quality of IC testing and reduce cost. Built-in self-test (BIST) is a primary self-test methodology and is widely used for testing VLSI circuits. This method configures circuits for testing itself, with the advantage of low test complexity, short test time, high fault coverage rate and so on. It will be a very important direction for future research. It includes test-pattern generators and output response analyzer. To test-pattern generators, Linear Feedback Shift Registers (LFSRs) becomes the mainstream, mainly due to its simple structure and high sequence coverage rate[1].

Reversible logic is of major interest in low power CMOS design and quantum computing [2-3]. Reference [4] presents primary reversible sequential elements such as D latch, JK latch and D Flip_Flop, etc. LFSR is an important sequential circuit for Design for Test.

LFSRs are widely used in DFT and BIST. For compressing the amount of test data, pseudo random binary test sequences are generated by LFSRs. With minimum length feedback polynomial LFSR can faster generation of binary sequences than based on linear congruential equations. Output data of LFSRs is compressed by a polynomial division process[5]. Undoubtedly, LFSR is known to be an extremely simple and fast way of generating a pseudo-random sequence.

II. LFSR

Figure 1 and Figure 2 show a typical internal and external XOR LFSR, respectively [6]. n denotes the length of the LFSR. $\phi_0 \cdots \phi_n$ are the binary coefficients. The characteristic polynomial of these LFSR is,

$$\phi(x) = \phi_n x^n + \cdots + \phi_1 x + \phi_0 \tag{1}$$

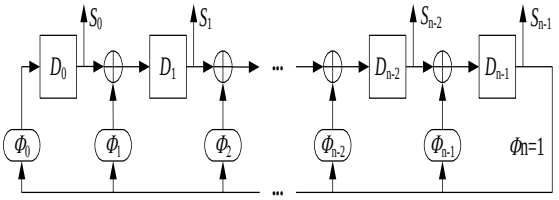

FIGURE I. A TYPICAL INTERNAL XOR LFSR.

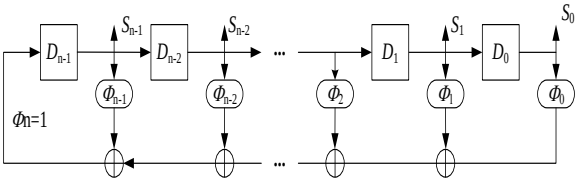

FIGURE II. A TYPICAL EXTERNAL XOR LFSR.

If ϕ_i is binary 1, it implies that a branch exists. In contrast if ϕ_i is binary 0, implies that no branch exists. In this case, input and output directly connect and corresponding XOR gate is removed.

A seed is the initial state of LFSRs which are run in autonomous mode to generate a set of test vector. Different initial seed will produce different test vectors. Input bits of LFSR are solutions of linear function for its previous state. It cycles through all possible states so that to generate random sequence. The period of the sequence is 2^n-1, where n is the number of shift registers in the LFSR.

III. RELATION OF LFSR SEQUENCE AND FEEDBACK POLYNOMIAL

LFSR by irreducible primitive polynomial can generate maximum length sequence[7-9]. The relation of Feedback polynomial and generation sequence is not complex. After t clocks, output state of D_i is denoted as $s_i(t)$, and other outputs are denoted as $s_{n-1}(0)$, $s_{n-1}(1),\ldots,s_{n-1}(j)$. The sequence generated is denoted as

$$G_{n-1}(x) = s_{n-1}(0) + s_{n-1}(1)x + \cdots + s_{n-1}(j)x^j + \cdots = \sum_{j=0}^{\infty} s_{n-1}(j)x^j \tag{2}$$

In equation 2, the x is time shift. For a internal XOR LFSR, when φn is one, output satisfy

$$s_{n-1}(j) = \sum_{i=0}^{n-1} \phi_i s_{n-1}(j-n+i) \tag{3}$$

It is brought into equation 2, we can have next equation.

$$G_{n-1}(x) = \frac{\sum_{i=0}^{n-1} \phi_i x^{n-1}[s_{n-1}(-n+i)x^{-n+i} + \cdots + s_{n-1}(-1)x^{-1}]}{1 + \sum_{i=0}^{n-1} \phi_i x^{n-i}} \tag{4}$$

IV. Design-for-Test of Reversible Sequential Circuits

D latch and D Flip_Flop are important elements for reversible sequential circuits. To realize reversible sequential circuits with testability, we presented primary reversible sequential elements, D Flip_Flop, in reference [10]. Considering reversible structure, we attempt to find a way to simplify garbage outputs functions. In response to this point, we present our own solutions in Figure 3. Compared with reference [4], cost of its realization is cut by one forth. A reversible D Flip_Flop is caused by this in Figure 3.

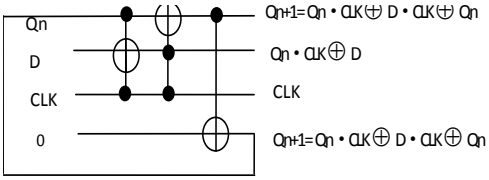

FIGURE III. OUR REVERSIBLE D LATCH.

A m-order can generate the longest sequence which is 2m-1 long. It is called M- sequence. According to the mode of primitive polynomial, LFSR circuit can generate the longest sequences, and also its structure is simple and its hardware cost is low. It is only made of m-bits shift registers and a series of XOR gates. LFSR states vector is defined as:

$$A(k) = a_1(k)a_2(k)a_3(k)\cdots a_m(k), k = 0,1,\cdots, a_i(k) \in \{0,1\} \tag{5}$$

To external-XOR LFSR, its state vectors are defined as follow:

$$\begin{bmatrix} a_1(k) \\ a_2(k) \\ a_3(k) \\ \vdots \\ a_m(k) \end{bmatrix} = \begin{bmatrix} c_1 c_2 c_3 & \cdots & c_{m-1} c_m \\ 1\ 0\ 0 & \cdots & 0\ \ 0 \\ 0\ 1\ 0 & \cdots & 0\ \ 0 \\ \vdots\ \vdots\ \vdots & & \vdots\ \ \vdots \\ 0\ 0\ 0 & \cdots & 1\ \ 0 \end{bmatrix} \begin{bmatrix} a_1(k-1) \\ a_2(k-2) \\ a_3(k-3) \\ \vdots \\ a_m(k-1) \end{bmatrix} \tag{6}$$

On the basis of this idea, we are able to set up a reversible LFSR circuit to generate pseudo-random variables with the reversible D flip-flop in reference [10]. For example four bits LFSR, its primitive polynomial is $\varphi(x)=x^4+x+1$. We exploit its LFSR pseudo-random sequences generator as show in figure 4. Table 1 lists a set of outputted pseudo-random sequences, when initial vector is 0001. We get 2^4-1 different kinds of vectors (a total of fifteen).

TABLE I .TABLE OF TEST PATTERNS FOR FOUR BITS LFSR.

Q0	Q1	Q2	Q3
1	0	0	0
0	1	0	0
0	0	1	0
1	0	0	1
1	1	0	0
0	1	1	0
1	0	1	1
0	1	0	1
1	0	1	0
1	1	0	1
1	1	1	0
1	1	1	1
0	1	1	1
0	0	1	1
0	0	0	1
1	0	0	0

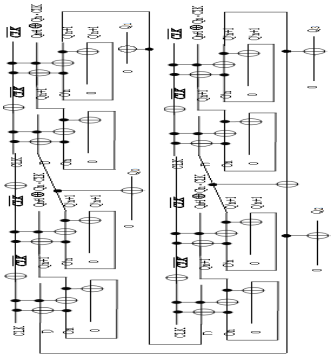

FIGURE IV. REVERSIBLE CIRCUIT FOR FOUR BITS LFSR.

V. Experimental Results

We have implemented our method in spice. Table 2 lists the number of generated pseudo-random sequences for reversible LFSR and general LFSR circuits with different length. For each scheme, two things are shown, the number of vector generated and size of the LFSR. As can be seen, for reversible LFSR, the ideal results are obtained.

TABLE II .PSEUDO-RANDOM TESTING RESULTS.

LFSR length	the number of pseudo-random vectors	
	Reversible LFSR	General LFSR
4	15	15
5	15	15
36	850	850
41	1200	1200
41	2550	2550

VI. Conclusions

In order to realize Design for Test in reversible circuits, we gave out the structure of reversible LFSR. It achieves the maximum length pseudo-random sequence.

ACKNOWLEDGMENTS

This research was supported in part by Key Fund Project of Heilongjiang Provincial Department of Education (No. 12541604).

REFERENCES

[1] Xinhui Zhang, C.I.H Chen, A. Chakravarthy. Structure Design and Optimization of 2D LFSR-Based Multisequence Test Generator in Built-In Self-Test. IEEE Trans. Instrum. Meas. pp.651-663, 2008.

[2] Li Zhiqing, Chen Hanwu, Xu Baowen. (). A fast algorithm for synthesis of quantum reversible logic circuits. Chinese Journal of Computers. pp. 1291-1303, 2009.(in China)

[3] Zilic Z, Radecka K, Kazamiphur A. Reversible circuit technology mapping from non-reversible specifications. Proceedings of the conference on Design, Automation and Test in Europe, France: IEEE Computer Society Press. pp.558-563,2007.

[4] Chuang M L, Wang C Y. Synthesis of reversible sequential elements. Proceedings of Asia and South Pacific Design Automation Conference, Japan: IEEE Computer Society Press. pp.420-425 , 2007.

[5] Hong-Sik Kim, Sungho Kang. Increasing encoding efficiency of LFSR reseeding-based test compression. Harmondsworth: IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems. pp.913-917, 2005.

[6] M. Dewar, D. Panario. Linear transformation Shift Regsters. IEEE Transactions on information theory. pp.2047-2052, 2003.(In Russian)

[7] A. K. Panda, P. Rajput, B. Shukla. FPGA Implementation of 8, 16 and 32 Bit LFSR with Maximum Length Feedback Polynomial using VHDL. International Conference on Communication Systems and Network Technologies. pp.769-773, 2012.

[8] E. I. Milovanovic, I. Z. Milovanovic, M. K. Stojcev. Concurrent Generation of Pseudo Random Numbers with LFSR of Galois Type. The 11th international conference on Telecommunicaion in Modern Satellite, Cable and Broadcasting Services, pp.61-64, 2013.

[9] S.Wang，Wenlong Wei，Srimat T. Chakradhar. A High Compression and Short Test Sequence Test Compression Technique to Enhance Compression of LFSR Reseeding. The 16th IEEE Asian Test symposium in Tokyo. pp.79-86, 2007.

[10] Hu Jing, Wen Dianzhong. Test-Synthesis method for Reversible Circuits. Journal of Convergence Information Technology. pp.245-251, 2012.