International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 7, Issue 1 (May 2013), PP. 109-115

Power Optimization of Linear Feedback Shift Register Using Clock Gating

Yasmeen Khan
Assistant Professor, Department of Electronics & Communication Engineering
Jagannath University,
Chaksu, Jaipur (Raj.), India Pin 303901.

Abstract:- A modified Linear Feedback Shift Register is designed in which power consumption reduction by deactivating the clock signal to Flip Flop when the output signal is same as input signal. The power consumption of the new LFSR is reduced due to the reduced switching of Flip Flop To verify, the maximum, minimum and average

Keywords:- LFSR, Optimization,Low Power, test Patterns

I. INTRODUCTION

TODAY, pseudo-random bit generators (PRBGs) are widely used in many electronic equipment. A good PRBG must be characterized by repeatability and randomness. Today, hardware implementation of the PRBGs is almost always made up of the well-known linear-feedback shift register (LFSR) whose generic circuit is reported. This circuit is very simple to be implemented, but since the clock-path of all flip-flops (FFs) toggle at every clock cycle, they consume a significant amount of power. In this paper, we present the gated clock design approach for LFSRs which can lead to power reduction without complicating the traditionally simple topology.

The main challenging areas in VLSI are performance, cost, testing, area, reliability and power. These demands for portable computing devices and communications system are increasing rapidly. These applications require low power dissipation for circuit implementation. The power dissipation during test mode is 200% more than the normal mode. Hence it is important aspect to optimize power during testing. Power optimization is one of the main challenges.

There are various factors that affect the cost of chip like packaging, application, testing. In VLSI, according to thumb rule 5000 of the total integrated circuits cost is due to testing. During testing two key challenges are:

- Cost of testing that can't be scaled.
- Engineering effort for generating test vectors increases as complexity of circuit increases. Based on 1997 SIA data, the upper curve shows the fabrication cost of transistor and lower curve shows the testing cost of transistor. Figure 1 shows that the fabrication cost transistor decreases over the decades according to but the testing cost as constant.

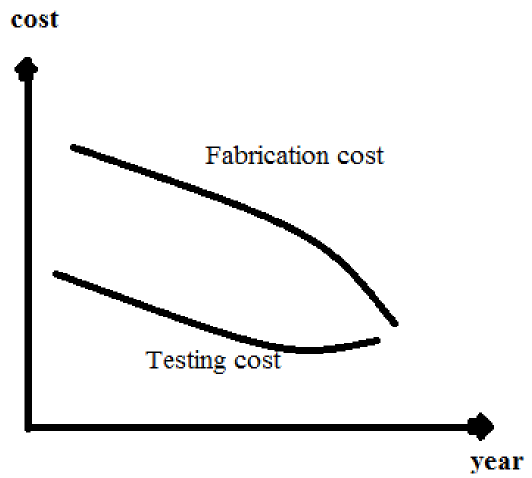


Fig.1 Fabrication and testing Cost curve

There are main two sources of power dissipation in digital circuits; these are static and dynamic power dissipation. Static power dissipation is mainly due to leakage current and its contribution to total power dissipation is very small. Dynamic power dissipation is due to switching i.e. the power consumed due to short circuit current flow and charging of load capacitances is given by equation:

P= 0.5 VDD 2E(SW)CL fclk

Where **VDD** is supply voltage, **E(SW)** is the average number of the main challenges. Output transitions per fclk Is the clock frequency and CL is the physical capacitance at the output of the gate. Dynamic power dissipation contributed to total power dissipation. The above equation shows the dynamic power depends on three parameters: Supply voltage, Clock frequency, switching activity. Power reduction using the switching activity doesn't degrade the performance of the circuit.

During testing large power is dissipated compare to the normal mode. This is due to lack of correlation between the Successive test patterns generated by ATPG or LFST and this large power dissipation cases following effects:

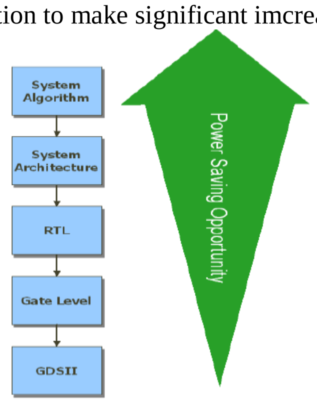
- The increased power may be responsible for cost, reliability, performance verification, autonomy and technology.
- Low power dissipation during test application is thus becoming an equally important figure of merit in.

For complex circuits we use hierarchical approach. The advantage of hierarchical approach is that every block is tested separately. Test input is given to each block and output is observed and verified. DFT (Design for Testability) is the action of placing features in a chip design process to enhance the ability to generate vectors, achieve a 3

measured quality level or reduce cost of testing. The conventional DFT approaches use scan and BIST. In this paper a modified low power LFSR are used in which the number of transitions of test pattern are reduced testing.

II. CLOCK GATING AT REGISTER TRANSFER LEVEL

Power should be optimized at all stages, but it is generally convenient to address it after Register Transfer Level (RTL).RTL clock gating is the most commonly used optimization technique for improving power consumption, but depends critically on how well a design is clock gated. At this point in the design flow, designer has flexibility in the implementation to make significant imcreament in the energy saving.



VARIOUS TYPES OF LFSR:

Fibonacci LFSRs :

In a 16-bit Fibonacci LFSR the feedback tap numbers in white correspond to a primitive polynomial so the register cycles through the maximum number of 65535 states excluding the all-zeroes state. The state shown, 0xACE1 (hexadecimal) will be followed by 0x5670.

The bit positions that affect the next state are known as taps. In the diagram the taps are [16,14,13,11]. The rightmost bit of the LFSR is called the output bit. The taps are XOR'd sequentially with the output bit and then fed back into the leftmost bit. The sequence of bits in the rightmost position is known as output stream.

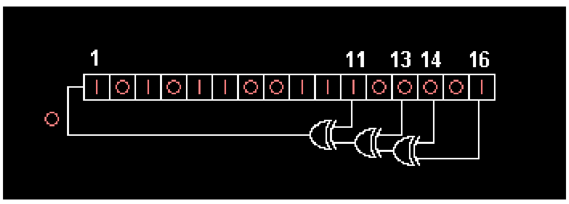


Fig.3 bit Linear Feedback Shift Register.

A maximum-length LFSR produces an m-sequence unless it contains all zeros, in which case it will never change. As the XOR based feedback in an LFSR, one can also use XNOR This function is an affine map, not a linear map, but it results in an equivalent polynomial counter whose state of this counter is the complement of the state of an LFSR. A state with all ones is illegal when using an XNOR feedback, same as a state with all zeroes is illegal when using XOR. This state is considered illegal because the counter would remain "locked-up" in this state.

The sequence of numbers generated by an LFSR or its XNOR counterpart can be considered a binary numeral system just as valid Gray code or the binary code. The arrangement of taps for feedback in an LFSR can be expressed in finite field arithmetic as a polynomial mod. This means that the coefficients of the polynomial must be one's or Zeroes. This is considered as the feedback polynomial or characteristic polynomial. For example, if the taps are at the 16th, 14th, 13th and 11th bits (as shown), the feedback polynomial is The 'one' in the polynomial does not correspond to a tap — it corresponds to the input to the first bit (i.e. x0, which is equivalent to 1). The powers of the terms represent the tapped bits, counting from the left. The first and last bits are always connected as an input and output tap respectively. There can be more than one maximum-length tap sequence for a given LFSR length once one maximum-length tap sequence .

<u>Galois LFSRs:</u>

An LFSR in Galois configuration, which is also known as modular, internal XORs as well as one-to-many LFSR, is an alternate structure that can generate the same output data as a conventional LFSR. In this configuration, when the system is clocked, bits that are not taps are shifted one position to the right unchanged. The taps, on the other hand, are XOR'd with the output bit before they are stored in the next position. The new output bit is the next's input bit. when the output bit is zero all the bits in the register shift to the right unchanged, and the input bit becomes zero. When the output bit is one, the bits in the tap positions, and then the entire register is shifted to the right and the input bit becomes 1.

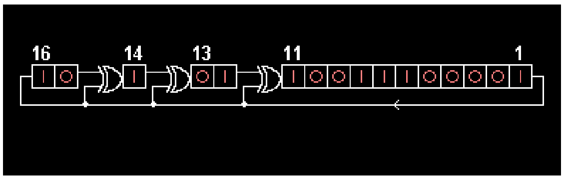


Fig.4 Galois LFSRs

A 16-bit Galois LFSR. The register numbers in white correspond to the same primitive polynomial as the Fibonacci example but are counted in reverse to the shifting direction. This register also cycles through the maximal number of 65535 states excluding the all-zeroes state. The state ACE1 hex shown will be followed by E270 hex.To generate the same output stream, the order of the taps is the counterpart (see above) of the order for the conventional LFSR, otherwise the stream will be in reverse. Note that the internal state of the LFSR is not necessarily the same. The Galois register shown has the same output stream as the Fibonacci register in the first section. Galois LFSRs do not concatenate every tap to produce the new input (the XOR'ing is done within the LFSR and no XOR gates are run in serial, therefore the propagation times are reduced to that of one XOR rather than a whole chain), thus it is possible for each tap to be computed in parallel, increasing the speed of execution.

<u>Non-binary Galois LFSR:</u>

Binary Galois LFSRs can be generalized to any q-ary alphabet {0, 1, ... , q − 1}. In Non binary, the XOR component is generalized to addition modulo-q, and the feedback bit is multiplied by a q-ary value which is constant for each specific tap point. In the binary case, where the feedback is multiplied by either 0 or 1.

III. BACK GROUND BEHIND PROJECT

The important challenging areas in VLSI is performance, cost testing, area, reliability and power. The demand for portable computing devices and communication system increasing rapidly. These applications require in low power dissipation for VLSI circuits. Power dissipation for testing is 200% more than simple mode. By using LFSR we can decrease power dissipation.

IV. HARDWARE IMPLEMENTATION:

Normal LFSR:

A linear feedback shift register is a shift register whose input bit is a linear function of its previous state. The only linear functions of single bits are XOR and inverse-XOR, thus it is a shift register whose input bit is driven by the XOR of some bits of the overall shift register value. As shown in Fig., it is obtained with an array of FF's with a linear feedback performed by several XOR gates. LFSR's are very easy to implement.

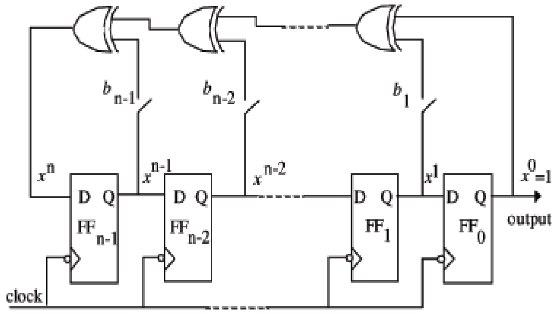


Fig.5 traditional LFSR

.

The taps of an LFSR can be represented as a polynomial mod. It shows the coefficients of polynomial must be 1's or 0's.For example, if the taps are at the 16th, 14th, 13th and 11th bits (as shown), the feedback polynomial is The 'one' in the polynomial does not correspond to a tap — it corresponds to the input to the first bit. The powers of the terms represent the tapped bits, counting from the left. The first and last bits are always connected as an input and tap respectively.

Clock Gating LFSR:

To reduce power consumption in a digital syste dynamic power management (DPM) is often used. The DPMs strategy consists in disabling the logic circuits that are not performing functional operations during a particular time, & reducing power consumption. At circuit level, this strategy is applied by the so-called "gated clock" approach which disables the clock of FFs when output is same as input, activating the FF only when the input signal is different from the actual output value. This approach is perfectly compatible with a LFSR only adding some extra.

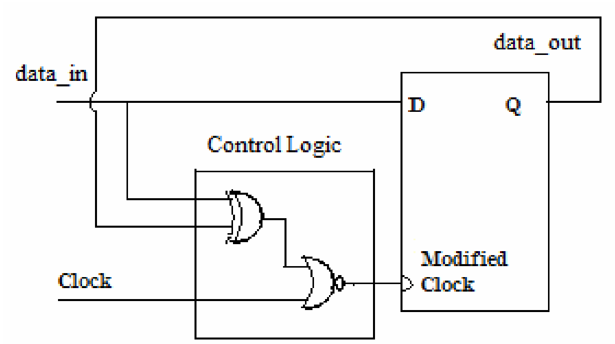


Fig.6 Gate clock based synchronization respect input and output value of FF.

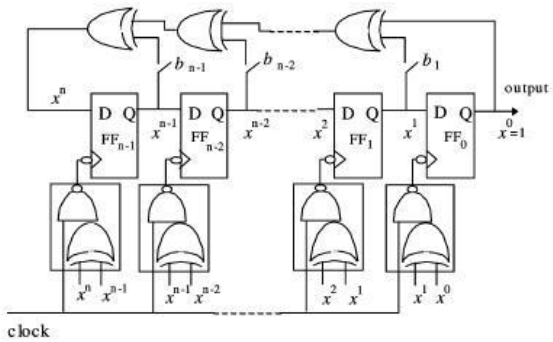


Fig.7 Gate-clock n-bit LFSR

V. APPLICATION OF LFSR

LFSRs can be implemented in hardware, and this makes them useful in applications that require very fast generation of a pseudo-random sequence. LFSRs have also been used for generating an approximation of white noise in various programmable sound generators.

Uses as counters:

The repeating sequence of states of an LFSR allows it to be used as a clock divider, or as a counter when a non-binary sequence is acceptable as is often the case where computer index or framing locations need to be machine-readable. LFSR counters have simpler feedback logic than natural binary counters or Gray code counters, and it can operate at higher clock rates. However it is necessary to ensure that the LFSR never enters an all-zeros state. One can obtain any other period by adding to an LFSR that has a longer period some logic that shortens the sequence by skipping some states.

Uses in cryptography:

LFSRs have long been used as pseudo-random number generators for use in stream ciphers, due to the ease of construction from simple electromechanical or electronic circuits, long periods, and very uniformly distributed output streams. An LFSR is a linear system, leading to fairly easy cryptanalysis. For example, given a stretch of known plaintext and corresponding ciphertext, an attacker can intercept and recover a stretch of LFSR output stream used in the system described, and from that stretch of the output stream can construct an LFSR of minimal size that simulates the intended receiver by using the Berlekamp-Massey algorithm. This LFSR can then be fed the intercepted stretch of output stream to recover the remaining plaintext.
Three general methods are employed for the reduction of this problem in LFSR-based stream ciphers:

- Non-linear combination of several bits from the LFSR state;
- Non-linear combination of the output bits of two or more LFSRs;
- Irregular clocking of the LFSR, as in the alternating step generator.

Uses in digital broadcasting and communications:

<u>Scrambling:</u>

To prevent short repeating sequences from forming spectral lines that may complicate symbol tracking at the receiver or interfere with other transmissions, linear feedback registers are often used to "randomize" the transmitted bit stream. This randomization is removed at the receiver after demodulation. When the LFSR runs at the same rate as the transmitted symbol stream, this technique is referred to as scrambling. When the LFSR runs considerablyfaster than the symbol stream, expanding the bandwidth of the transmitted signal, this is direct-sequence spread spectrum.

Neither scheme should be confused with encryption nor do decipherment, scrambling and spreading with LFSRs not protect the information from eavesdropping.
Digital broadcasting systems that use linear feedback registers:

- ATSC Standards (digital TV transmission system)
- DAB (Digital Audio Broadcasting system – for radio)
- DVB-T (digital TV transmission system)
- NICAM (digital audio system for television)

Other digital communications systems using LFSRs:

- IBS (INTELSAT business service)
- IDR (Intermediate Data Rate service)
- SDI (Serial Digital Interface transmission)
- Data transfer over PSTN
- CDMA cellular telephony
- 100BASE-T2 "fast" Ethernet scrambles bits using an LFSR
- 1000BASE-T Ethernet, the most common form of Gigabit Ethernet, scrambles bits using an LFSR

Other uses:

The German time signal DCF77, in addition to amplitude keying, employs phase-shift keying driven by a 9-stage LFSR to shows the increment the accuracy of received time and the robustness of the data stream in the presence of noise.

The Global Positioning System uses an LFSR to rapidly transmit a sequence that indicates high-precision relative time offsets.LFSRs are also used in Communications System Jamming systems in which they are used to generate pseudo random noise to raise the noise floor of a target communication system.

VI. SIMULATION

Normal LFSR:

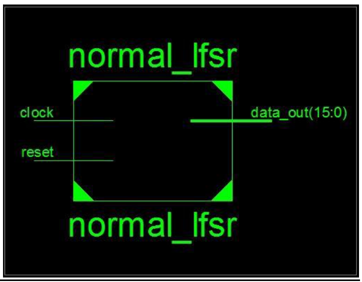


Fig.8 RTL of Normal LFSR

Fig 9 waveform of normal LFSR

LFSR using Clock gating:

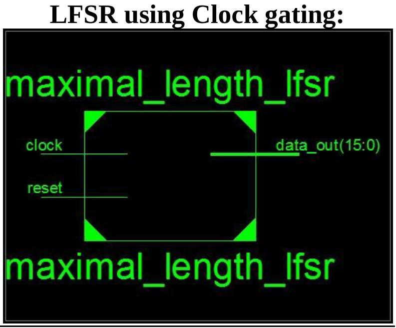


Fig.10 RTL of maximal LFSR

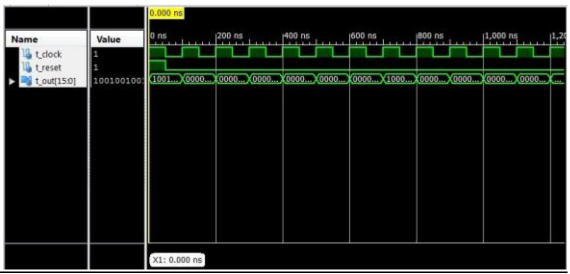


Fig.11 waveform of maximal LFSR

VII. RESULT AND CONCLUSION

In order to evaluate the power reduction obtained by applying clock gating in LFSR, we have evaluated the power consumption in 16 bit Traditional LFSR and power consumption in 16 bit LFSR with clock gating for same input vector and same clock cycles. VHDL code of traditional 16 bit LFSR was simulated in Xilinx 13.2 ISE Navigator and then VHDL code of 16 bit LFSR with gated clock was simulated and synthesized and the Xpower was obtained using Xilinx XPower Analyzer.

The results obtained from the Xilinx 13.2 implementation with the device in which, we have generated NCD, PCF, SAIF files after the post simulation. Xpower is used to calculate the with the simulation file. Reduced power Linear Feedback Shift Register with gated clock is here designed. There is **52% reduction** in Dynamic power, **1.5% reduction** in total power achieved. In contrast to the above results, that may be due to power consumed in initial transitions and that is in order of mili-watts, which is too small as compared to power reduction in Dynamic power and total power.

	Without Clock Gating (mW)	With Clock Gating (mW)
Total	208.91	205.94
Dynamic	5.48	2.59
Quiescent	203.43	203.35

Table.1 Comparison between 16 bit Traditional LFSR and16 bit clock gate LFSR.

ACKNOWLEDGEMENT

I would like to acknowledge and extend my heartfelt gratitude to the following persons who have made the completion of this paper possible:

1. Dr. Y.S Shishodiya, ProVice Chancelor, Jagannath University,Chaksu,Jaipur(Raj.)
2. Dr. Y.C Bhatt, Director, Jagannath Institute of Management Technology,Jaipur(Raj.)
3. Ramesh Bharthi, Head of the department, Electronics and Communication Branch, Jagannath University Chaksu,Jaipur(Raj.)
4. Rajneesh Goyal,Assitant Professor Jagannath Institute of Management Technology Jaipur(Raj.)

REFERENCES

[1]. E. Atoofian, S. Hatami, Z. Nawabi, M. Alisaface and A. afzali-khusa “ A new power scan path architecture”

[2]. The national technology road map for semiconductor (ITRS). Semiconductor industry association.

[3]. Dr. K.Gunavathi, Dr. K. Paramshivam, Ms P. Subashini Lavanya, M. Umamageswaran, “ A novel BIST TPG for testing of VLSI circuit.

[4]. Mohammad Tehranipoor, Mehrdad Nourani, Nisar Ahmed”, low transition LFSR for BIST based applications”.

[5]. Michael N. Bushnell, Vishwani D. Agawal”, essential of electronic testing for digital memory and mix signal VLSI circuits”

[6]. Fulvio corno, Paolo prinettom, Matteo sonzar Eorda “testability analysis and ATPG on behavioral RT-level VHDL”.

[7]. F.Corno, P. Prinetto, R.Rebuadengo, M.Sonza Reorda” A test pattern generation methodology

[8]. Jinkyu Lee and Nur A. Touba," LFSR-Reseeding Scheme Achieving Low-Power dissipation during Test," IEEE transactions on computer- aided design of integrated circuits and systems.

[9]. Shilesh Malliyoor, Chao You," Comparison of hardware implementation and power consumption of low-power multiple output linear feedback shift register,".

[10]. Yervant Zorianl, Sujit Dey, Michael J. Rodgers "Test of Future System-on-Chips"ICCAD.