Concepts of Primitive Polynomial and Galois Field in Designing More Randomize PN Sequence Generators for Maximum Fault Coverage in Modern VLSI Testing

Priyanka Shrivastava, Prashant Purohit, Pushpraj Singh Tanwar, Harishanker Shrivastava

Abstract— This paper deals with the vital role of primitive polynomials for designing PN sequence generators. The standard LFSR (linear feedback shift register) used for pattern generation may give repetitive patterns. Which are in certain cases is not efficient for complete test coverage. The LFSR based on primitive polynomial generates maximum-length PRPG.

Index Terms—1. LFSR (linear feedback shift register). 2. PRPG (Pseudo feedback shift register).3 Primitive polynomial 4. Galois field.

I. INTRODUCTION

An LFSR is a shift registers that, when clocked, advances the signal through the register from one bit to the next most-significant bit (figure1). Some of the outputs are combined in exclusive-OR configuration to form a feedback mechanism. A linear feedback shift register can be formed by performing exclusive-OR on the outputs of two or more of the flip-flops together and feeding those outputs back into the input of one of the flip-flops as shown in Figure 2.

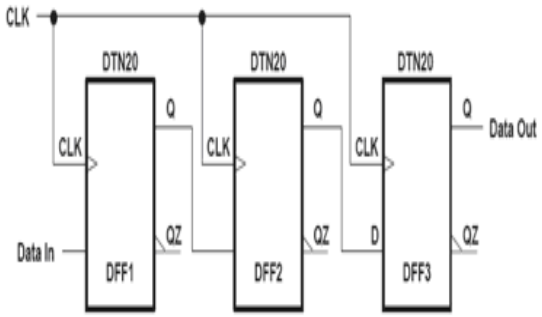


Fig. 1. 3-Bit Shift Register

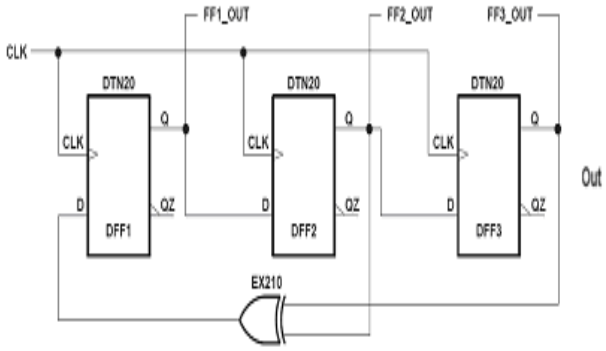


Fig. 2 Linear Feedback Shift Register

II. PROCEDURE FOR PAPER SUBMISSION

A. Pseudo Random Pattern Generator (PRPG)

Linear feedback shift registers make extremely good pseudorandom pattern generators. When the outputs of the flip-flops are loaded with a seed value (anything except all 0s, which would cause the LFSR to produce all 0 patterns) and when the LFSR is clocked, it will generate a pseudorandom pattern of 1s and 0s. The only signal necessary to generate the test patterns is the clock.

B. Standard LFSR

An standard LFSR is shown in figure 3. It consists of n D flip-flops and a selected number of exclusive-OR (XOR) gates. Because XOR gates are placed on the external feedback path, the standard LFSR is also referred to as an external-XOR LFSR.

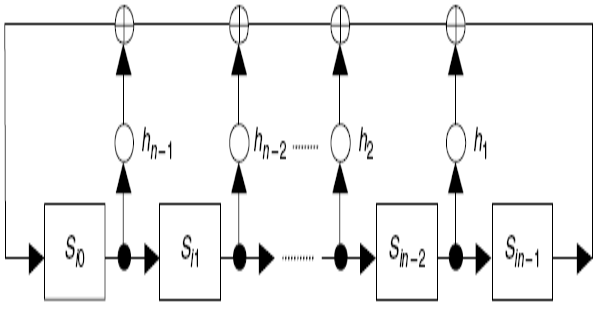


Fig. 3 N Stage (External –Xor) Standard LFSR

Manuscript Received on September 2014.

Miss Priyanka Shrivastava, Department of EC (Digital Communication), RGPV, Radharaman Institute of Technology & Science, Bhopal, India.

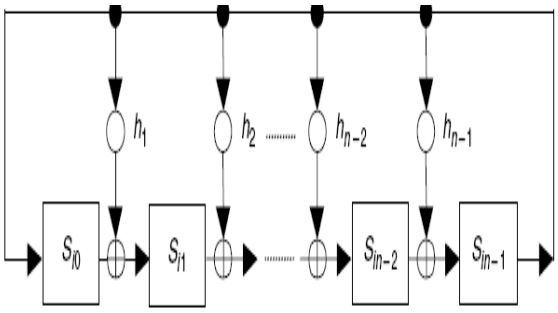
Prof. Prashant Purohit, Department of EC, RGPV, Radharaman Institute of Technology & Science, Bhopal, India.

Prof. Pushpraj singh Tanwer, Department of EC, RGPV, Radharaman Institute of Technology & Science, Bhopal, India.

Prof. Harishankar Shrivastava, Department of EC, RGPV, Radharaman Institute of Technology & Science, Bhopal, India.

C. Modular LFSR

The modular LFSR runs faster than its corresponding standard LFSR, because each stage introduces at most one XOR-gate delay. An n stage modular LFSR is shown in figure 4. It is also referred to as modular or internal-LFSR.



The internal structure of the n-stage LFSR in each figure can be described by specifying a characteristic polynomial of degree n, f(x), in which the symbol hi is either 1 or 0, depending on the existence or absence. Let Si represent the contents of the n-stage LFSR after ith shifts of the initial contents S0, of the LFSR, and let Si(x) be the polynomial representation of Si.

Then, Si(x) is a polynomial of degree n−1, where:

$Si(x) = Si0 + Si_1x + Si_2x^2 + Si_3{}^{x3} + Si_4\,x^4 + \ldots\ldots\ldots + Si_{n-2}x^{n-2} + Si_n.1x^{n-1.}$

of the feedback path, where

$$f(x) = 1 + h_1x + h_2x^2 + \cdots + h_{n-1}x^{n-1} + x^n$$

If T is the smallest positive integer such that f(x) divides 1+xT, then the integer T is called the period of the LFSR. If T = 2n −1, then the n-stage LFSR generating the

$$\frac{x+1}{x^2+x+1} = \frac{x+1}{x^2+x+1} \pmod 2$$

$$\frac{x^2+1}{x^2+x+1} = 1 + \frac{x}{x^2+x+1} \pmod 2$$

$$\frac{x^3+1}{x^2+x+1} = x+1 \pmod 2.$$

maximum-length sequence is called a maximum-length LFSR. Consider the four-stage standard and modular LFSR shown in Figure 5(a) and figure 5(b), below. The characteristic polynomials f(x) used to construct both LFSR are $1+x^2+x^4$ and $1+x+x^4$, respectively.

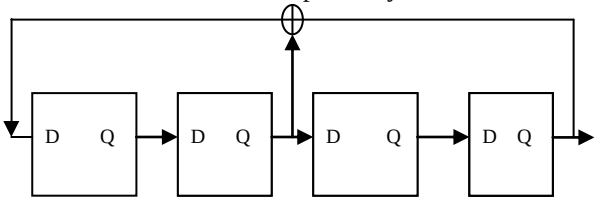


Fig. 5 (a) 4-Bit Standard LFSR

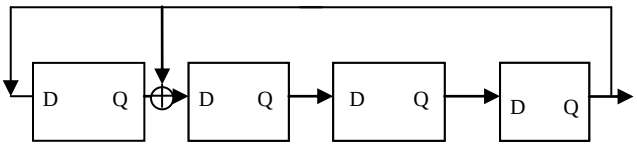


Fig. 5 (b) 4-Bit Modular LFSR

The test sequences generated by each LFSR, when its initial contents, S0, are set to {0001}.

PN Sequence for fig.5(a)	PN sequence for fig.5 (b)
0 0 0 1	**0 0 0 1**
1 0 0 0	1 1 0 0
0 1 0 0	0 1 1 0
1 0 1 0	0 0 1 1
0 1 0 1	1 1 0 1
0 0 1 0	1 0 1 0
0 0 0 1	0 1 0 1
1 0 0 0	1 1 1 0
0 1 0 0	0 1 1 1
1 0 1 0	1 1 1 1
0 1 0 1	1 0 1 1
0 0 1 0	1 0 0 1
0 0 0 1	1 0 0 0
1 0 0 0	0 1 0 0
0 1 0 0	0 0 1 0

III. PRIMITIVE POLYNOMIAL

A primitive polynomial is a polynomial that generates all elements of an extension field from a base field. Primitive polynomials are also irreducible polynomials. For any prime or prime power q and any positive integer n, there exists a primitive polynomial of degree n over GF(q).

There are

$$a_q(n) = \frac{\Phi(q^n - 1)}{n} \quad \ldots\ldots\ldots \text{(i)}$$

Primitive polynomials over GF (q).

Where $a_q(n)$ is the totient function. A polynomial of degree n over the finite field GF (2) (i.e., with coefficients either 0 or 1) is primitive if it has polynomial order 2^n-1. For example, $1+x+x^2$has order 3 since

Putting q=2 in equation (i) the numbers of primitive polynomials over GF(2) are

$$a_2(n) = \frac{\Phi(q^n - 1)}{n} \quad \ldots\ldots\text{(ii)}$$

giving 1, 1, 2, 2, 6, 6, 18, 16, 48, ... for n= 1,2.... The following table lists the primitive polynomials (mod 2) of orders 1 through 5.

n	Primitive polynomials
1	1+x
2	$1+x+x^2$
3	$1+x+x^3$, $1+x^2+x^3$
4	$1+x+x^4$,$1+x^3+x^4$
5	$1+x^2+x^5$, $1+x+x^2+x^3+x^5$, $1+x^3+x^5$, $1+x+x^4+x^3+x^5$, $1+x^2+x^3+x^4+x^5$ $1+x+x^2+x^4+x^5$,

A primitive polynomial of degree n over Galois field GF(2), p(x), as a polynomial that divides $1+X^T$, but not 1+Xi for any integer i < T, where T = 2n -1.A primitive polynomial is irreducible. Because T = 15 = 14 -1.The characteristic Polynomial, $f(x) = 1+x+x^4$, used to construct Figure 5(b) is a primitive polynomial; thus the modular LFSR is a maximum-length LFSR.

Let $R(X) = F(X)^{-1} = X$ n $F(X^{-1})$ then R(X) and F(X) are reciprocal and a reciprocal polynomial of primitive polynomial is also primitive. Hence polynomials$1+x+x^4$,$1+x^3+x^4$ are primitive.

IV. GALOIS FIELD

A finite field is a field with a finite field order (i.e., number of elements), also called a Galois field. The order of a finite field is always a prime or a power of a prime . For each prime power, there exists exactly one (with the usual caveat that "exactly one" means "exactly one up to an isomorphism") finite field GF (p^n). GF(p) is called the prime field of order p, and is the field of residue classes modulo p, where the p elements are denoted 0, 1, ...,(p-1). a=b in GF(p) means the same as a=b(mod p). However, that 2x2=0(mod4)in the ring of residues modulo 4, so 2 has no reciprocal, and the ring of residues modulo 4 is distinct from the finite field with four elements. Finite fields are therefore denoted GF(p^n), instead of GF(k), where k= p^n. The finite field GF(2) consists of elements 0 and 1 which satisfy the following addition and multiplication tables.

+	0	1
0	0	1
1	1	0
X	0	1
0	0	0
1	0	1

If a subset S of the elements of a finite field F satisfies the axioms above with the same operators of F, then S is called a subfield. Finite fields are used extensively in the study of error-correcting codes.

V. HELPFUL HINTS

When n>1, GF(p^n) can be represented as the field of equivalence classes of polynomials whose coefficients belong to GF(p). Any irreducible polynomial of degree n yields the same field up to an isomorphism. For example, for GF(2^3), the modulus can be taken as x^3+x^2+1 or x^3+x+1. Using the modulus x^3+x^2+1, the elements of GF(2^3)can be written as written 0, x^0,x^1, x^2 .....and can be represented as polynomials with degree less than 3. Now consider the following table which contains several different representations of the elements of a finite field. The columns are the power, polynomial representation, triples of polynomial representation coefficients (thevector representation), and the binary integer corresponding to the vector representation (the regular representation).

power	polynomial	vector	regular
0	0	**(000)**	**0**
x^0	1	**(001)**	**1**
x^1	x	**(010)**	**2**
x^2	x^2	**(100)**	**4**
x^3	x+1	**(011)**	**3**
x^4	X^2+1	**(110)**	**6**
x^5	x^2+ x +1	**(111)**	**7**
x^6	x^2 +1	**(101)**	**5**

The set of polynomials in the second column is closed under addition and multiplication modulox^3+x+1, and these operations on the set satisfy the axioms of finite field. This particular finite field is said to be an extension field of degree 3 of GF(2), written GF(2^3), and the field GF(2) is called the base field of GF(2^3). If an irreducible polynomial generates all elements in this way, it is called a primitive polynomial. For any prime or prime power q and any positive integer n, there exists a primitive irreducible polynomial of degree n over GF(q). For any element c nof GF(q), c^q=c, and for any nonzero element d of GF(q),$d^{(q-1)}$=1. There is a smallest positive integer n satisfying the sum condition e+e+e+….(n times)=0 for some element e in GF(q). This number is called the field characteristic of the finite field GF(q). The field characteristic is a prime number for every finite field, and it is true that $(x+y)^p = x^p + y^p$ a finite field with characteristic p.

VI. CONCLUSION

Primitive polynomial and Galois field gives idea about the designing the LFSRs with maximum length pattern. The more the random pattern the more the fault coverage is possible for testing the VLSI chips. Hence it is useful to implement a PRPG (pseudo random pattern generator) based on primitive polynomials for efficient and exhaustive-pseudo random testing. Thus improves the performance of PRPG.

REFERENCES

1. A. Miczo, Digital Logic Testing and Simulation, Second Edition, John Wiley, 2003
2. Berlekamp, E. R. Algebraic Coding Theory. New York: McGraw-Hill, p. 84, 1968
3. B. Koenemann. LFSR-coded test patterns for scan de-signs. Proc. Euro. Test Conf., pages 237{242, 1991
4. B. Konemann, "LFSR-Coded Test Pattems for Scan Designs", European Test Conference, Munich, 1991.Vol. 10, No.1, pp. 73-82. 1999, pp.358-367.20f
5. Church, R. "Tables of Irreducible Polynomials for the First Four Prime Moduli." Ann. Math. 36, 198-209, 1935
6. Derbyshire, J. Prime Obsession: Bernhard Riemann and the Greatest Unsolved Problem in Mathematics. New York: Penguin, pp. 266-268, 2004.
7. Lidl, R. and Niederreiter, H. Introduction to Finite Fields and Their Applications, rev. ed. Cambridge, England: Cambridge University Press, 1994.
8. Mohamed H. El-Mahlawy, Pseudo-Exhaustive Built-In Self-resf for Boundary Scan, Ph.D. thesis, Kent University, U.K., 2000.
9. Michael L. Bushnell and Vishwani D. Agrawal, Essentials of Electronic Testing For Digital, Memory, & Mixed-Signal VLSI Circuits, Kluwer Academic Publishers, 2000.

10. N. K. Jha and S. Gupta, Testing of Digital Systems, Cambridge University Press, UK, 2003.
11. N.C. Lai, S.J. Wang, "A Reseedin Technique for LFSRBased BIST Applications", Asian test Symposium 2002, pp.200-205.
12. Peterson, W. W. and Weldon, E. J. Jr. Error-Correcting Codes, 2nd ed. Cambridge, MA: MIT Press, p. 476, 1972.
13. P.H. Bardell, W.H. McAnney, Parallel Pseudo-random Sequences for Built-In Test, Proc. Int. Test Conf., IEEE, 1984, pp. 302-308.
14. P. H. Bardell, W. H. McAnney, and J. Savir. Built-in test for VLSI: Pseudorandom techniques. 1987.