Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

On the Periodicity of Non-Maximal Length Linear Feedback Shift Register Sequences

Venkata Krishna Rao M,
Professor and Head,
Department of Electronics & Communication Engineering,
Vidya Jyothi Institute of Technology,
Hyderabad, India

***Abstract*—Pseudo-Noise (PN) sequences are widely used in, from simple applications such as clock dividers to complex applications such as spread spectrum communication systems. Among PN sequences, maximal length (m-)sequences are very popular for communications and ranging applications, due to their desirable properties. While m-sequences are available only in limited number of lengths, the non-maximal length (NML) sequences are available in varieties of lengths. It appears that the NMLS were not investigated into, to the extent they deserve. The author conjectures that several other (non-communications) applications might benefit from the NLM sequences. In this paper, generation and periodicity property of NLM sequences, corresponding to polynomials of degree 3 to 20 are investigated. The results are expected to create an interest among the researchers in exploring some new applications of NML sequences.**

Keywords— PN sequences, Reducible polynomials, Linear feedback shift register sequences, Mobius-Mu function, Euler-Phi function

I. INTRODUCTION

Pseudo-Noise (PN) sequences find applications in spread spectrum communication systems [1], radar [2], clock dividers [3], system identification [4,5,6,7,8], VLSI circuit testing [9,10], test-pattern generation and for signature analysis [11], scrambling in digital broadcasting and communications [12], cryptography [13] and programmable sound generators [14]. A special class of PN sequences, called the Binary Linear Feedback Shift Register (LFSR) Sequences are generated using a simple hardware i.e. shift register whose individual stage outputs are feedback to the input through a modulo-2 adder. The LFSRs with certain combinations of feedback connections give rise to sequences of maximum length i.e. $2^n - 1$, where n is the number of stages of the shift register. These sequences are called maximal sequences (m-sequences), which are preferred to non-maximal sequences in most of the real systems, due to their desirable properties. Accordingly, the non-maximal sequences were almost ignored and their properties were not explicitly discussed in the literature. The author conjectures that several other applications might benefit from non-maximal length sequences.

In this paper, the non-maximal length sequences generated by linear feedback shift register and their periodicity property are discussed in detail. The paper is organized as follows. In section I, the mathematical structure associated with LFSR sequence generator is discussed. The primitive irreducible polynomials and their connection to m-sequences is also discussed. Section III is dedicated to Non-maximal Length Shift Register (NMLSR) sequences. In this section, generation and periodicity property of NMLSR sequences corresponding to polynomials of degree 3 to 20 are investigated analytically. Section IV discusses the details of simulations and the results. Conclusions and scope of future work are presented in section V.

II. BINARY LINEAR FEEDBACK SHIFT REGISTER SEQUENCES

Let a binary polynomial $h(x)$ of degree n is given by

$$h(x) = h_0 x^n + h_1 x^{n-1} + \ldots + h_{n-1} x + h_n \qquad (1)$$

where $h_0 = h_n = 1$ and other coefficients $h_i \in \{0,1\}$. The polynomial $h(x)$ can also be represented as a binary vector $\boldsymbol{h} = (h_0, h_1, \ldots, h_{n-1}, h_n)$ expressed either in binary or in octal notation. The vector $\boldsymbol{h}$ or equivalently the polynomial $h(x)$ can be used to generate a binary sequence $\boldsymbol{a} = a_0, a_1, a_2, \ldots\ldots\ldots$ using an n-stage binary shift register circuit with a feedback tap connected to i-th stage if $h_i = 1$ for $0 < i \leq n$. Since $h_n = 1$, the n-th stage always has a connection. Thus $h(x)$ is said to be the generator polynomial of the sequence $\boldsymbol{a}$.

$$a_k = h_1 a_{k-1} + h_2 a_{k-2} + \cdots + h_n a_{k-n} \qquad (2)$$

A 5-stage linear feedback shift register circuit corresponding to the polynomial $x^5 + x^3 + 1$ is shown in Fig.1. If the current output is taken from the k^{th} stage, then $(k-1)^{st}$ is the previous stage, $(k-2)^{nd}$ is the second previous stage and so on. Now by dividing the given polynomial by x^5, we get the polynomial $1 + x^{-2} + x^{-5}$. Here a positive power means an advancement of a bit position, where as a negative power means a delay of the bit position. Thus both the polynomials represent the same shift register circuit. The former takes the reference stage at the right, while the latter considers the reference stage at the left. The binary vector corresponding to the polynomial $x^5 + x^3 + 1$ is (101001) which is 51 in octal notation.

The sequence $\boldsymbol{a}$ generated by the LFSR circuit initially loaded with a non-zero binary vector in Fig. 1 repeats every N bits. If the polynomial is a primitive irreducible, then the sequence length is maximized with a period of $N = 2^n - 1$,

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

where n is the number of stages of the shift register which is same as the degree of the generator polynomial . This sequence is popularly known as maximal length sequence (MLS) or m-sequence [15]. The sequences generated with different initial shift register states (i.e. initial content of shift register) are the same except for a cyclic shift. If the polynomial is reducible into factors, then $N < 2^n - 1$ and the sequences are called non-maximal length sequences (NMLS). The variable L is used to represent the length of NMLS and $L < N$.

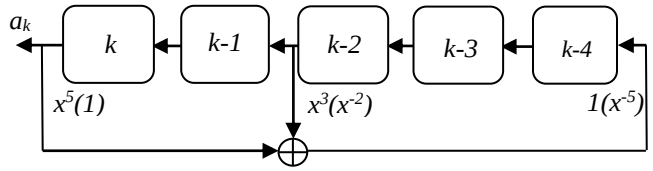

Fig. 1. A 5-stage linear feedback shift register with tap connections corresponding to the polynomial x^5+x^3+1 or $1+x^{-2}+x^{-5}$.

The m-sequences [15,16] have some desirable properties which make them unanimously preferred over m-sequences. The most important property is 2-level thumb-tack autocorrelation function and extremely low cross correlation function of the set of sequences corresponding to the generator polynomial of same degree. Whereas the m-sequences are available in limited number of lengths i.e. $N = 2^n - 1$, the NMLS are available in varieties of lengths.

For a given degree *n*, a polynomial must be irreducible if it has to generate either an m-sequence or a non-maximal length sequence (*nm*-sequence). Only the irreducible polynomials that are primitive generate m-sequences. For a given degree, the number of either *m*-sequences or *nm*-sequences available depends on the number of the primitive and non-primitive polynomials available. The number of such polynomials can be found using Möbius μ-function and Euler φ-function respectively as follows.

A. *Number of Irreducible Polynomials*

The number of irreducible polynomials modulo-2 of degree *n* is given by

$$\psi(n) = \frac{1}{n}\sum_{d/n} 2^d \, \mu\left(\frac{n}{d}\right) \tag{3}$$

where $\mu(.)$ is the Möbius μ-function [15] the sum is over all positive divisors of d of n. For $n= 8$, the divisors of 8 are $d = 1,2,4,8$, then $n/d = 8,4,2,1$ and $\mu(8/d) = 0,0,-1,-1$. Substituting in (3), we get $\psi(8) = 30$ i.e. there are 30 irreducible polynomials of degree 8. These are the LFSR sequences that can be generated using a shift register of 8 stages.

B. *Number of Primitive Polynomials*

The number of primitive polynomials modulo-2 of degree n is given by

$$\lambda(n) = \frac{\phi(2^n - 1)}{n} \tag{4}$$

where $\phi(.)$ is the Euler φ-function [15]. For $n= 8$, $\phi(255) = \phi(3.5.17) = 2.4.16 = 128$. Substituting in (4), we get $\lambda(n) = 128/8 = 16$. i.e. there are 16 primitive polynomials of degree 8. This means out of 30 irreducible polynomials of degree 8, only 16 polynomials are primitive which give rise to m-sequences of length 255. The remaining 14 polynomials are not primitive and generate non-maximal length sequences having lengths $L < 255$. Table I gives the number of non-maximal length sequences as computed from (3) and (4). It may noted that for degrees 3,4,5,7,13,17 and 19, no non-maximal length sequences exist meaning that all irreducible polynomials are primitive only.

TABLE I. UMBER OF NONMAXIMAL LENGTH SEQUENCES FOR DEGREES 3 TO 20

Degree n	Number of irreducible polynomials $\psi(n)$	Number of maximal length sequences $\lambda(n)$	Number of non-maximal length sequences $\psi(n) - \lambda(n)$
3	2	2	0
4	2	2	0
5	6	6	0
6	9	6	3
7	18	18	0
8	30	16	14
9	56	48	8
10	99	60	39
11	186	176	10
12	335	144	191
13	630	630	0
14	1161	756	405
15	2182	1800	382
16	4080	2048	2032
17	7710	7710	0
18	14532	7776	6756
19	27594	27594	0
20	52377	24000	28377

III. NONMAXMIAL LENGTH SHIFT REGISTER SEQUENCES

In this section, the lengths of non-maximal length sequences for degrees 3 to 20 are computed. If the number $N = 2^n - 1$ has factors other than *1* and *N* itself, then both primitive and nonprimitive polynomials exist for the degree *n*.

Table II gives the lengths of maximal length sequences L for degrees 3 to 20. The third column gives the factors of L. These factors are nothing but the lengths of non-maximal length sequences. These factors (equivalently, the sequence lengths) are used as arguments in Euler φ-function to compute the number of sequences having these lengths. The maximal lengths *N* corresponding to *n*=3,5,7,13,17 and *19* i.e. 7, 31, 127, 8191, 131071 and 524287 are called *mersenne primes*.

Let us consider $n = 8$, then $N = 255$ which has factors: 1, 3, 5, 15, 17, 51, 85 and 255. The sequences generated by the irreducible polynomials of degree 8 must have one of the periods: 1, 3, 5, 15, 17, 51, 85 and 255. The case of 15 is ignored as it is already considered for lower degree *n*=4, *N*=15. As 3 and 5 are factors of 15, they are also ignored. There are 30 irreducible polynomials (please refer to Table I) which give rise to sequences of periods: 17, 51, 85 and 255. There are 16 m-sequences having length of 255

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

corresponding to 16 primitive polynomials. The remaining 14 sequences have lengths: 17, 51 and 85. The number of sequences having these lengths can be again found from (4). Thus $\phi(17) = 16$, $\phi(51) = 32$ and $\phi(85) = 64$, giving rise to $\lambda(.) = 16/8 = 2$, $\lambda(.) = 32/8 = 4$ and $\lambda(.) = 64/8 = 8$. Thus there are two sequences of length 17, four sequences of length 51 and eight sequences of length 85, thus making a total of 14 non-maximal length sequences (please refer to Table III).

Similarly, for degree 6, $N = 2^6 - 1 = 63$ has factors sorted in ascending order: 1, 3, 7, 9, 21, 63. Out of these the lengths of 3 and 7 were already obtained from lower degrees 2 and 3 respectively. Since $\phi(9)/6 = 6/6 = 1$, there is one sequence of length 9 and since $\phi(21)/6 = 12/6 = 2$, there are two sequences of length 21. Similarly, $\phi(63)/6 = 36/6 = 6$, there are six sequences of length 63, which are m-sequences. Thus the total number of sequences obtained for degree 6 are 9, out of which three sequences are of non-maximal length. Samples of the actual sequences obtained through simulations are given in section IV.

TABLE II. MAXIMAL LENGTHS (L) AND FACTORS OF L FOR DEGREE 6 TO 20

Degree *n*	$N = 2^n - 1$	Factors of N
3	**7**	1.7
4	15	1.3.5.15
5	**31**	1.31 (Mersenne Prime)
6	63	1.3.7.9.21.63
7	**127**	1.127 (Mersenne Prime)
8	255	1.3.5.15.17.51.85.255
9	511	1.7.73.511
10	1023	1.3.11.31.33.93.341.1023
11	2047	1.23.89.2047
12	4095	1.3.5.7.9.13.15.21.35.39.45.63.65.91.105.117. 195.273.315.455.585.819.1365.4095
13	**8191**	1.8191 (Mersenne Prime)
14	16383	1.3.43.127.129.381.5461.16383
15	32767	1.7.31.151.217.1057.4681.32767
16	65535	1.3.5.15.17.51.85.255.257.771.1285.3855. 4369.13107.21845.65535
17	**131071**	1.131071 (Mersenne Prime)
18	262143	1.3.7.9.19.21.27.57.63.73.133.171.189.219. 399.511.513.657.1197.1387.1533.1971.3591. 4161.4599.9709.12483.13797.29127.37449. 87381.262143
19	**524287**	1.524287 (Mersenne Prime)
20	1048575	1.3.5.11.15.25.31.33.41.55.75.93.123.155.165. 205.275.341.451.465.615.775.825.1023.1025. 1271.1353.1705.2255.2325.3075.3813.5115. 6355.6765.8525.11275.13981.19065.25575. 31775.33825.41943.69905.95325.209715. 349525.1048575

The number of non-maximal length sequences of different lengths obtained for a given degree *n* are computed and listed in Table III for degrees 3 to 19. The sequence lengths for degree 20 are avoided due to space constraints, but can be computed from factors listed in Table II and using (4).

TABLE III. LENGTHS OF NONMAXMIAL LENGTH SEQUENCES (NMLS) FOR DEGREE 6 TO 20

Degree *n*	Period of NMLS	Number of NMLS	Total Number of NMLS
6	21 9	2 1	3
8	85 51 17	8 4 2	14
9	73	8	8
10	341 93 33 11	30 6 2 1	39
11	89 23	8 2	10
12	1365 819 585 455 315 273 195 117 105 91 65 45 39 35 13	48 36 24 24 12 12 8 6 4 6 4 2 2 2 1	191
14	5461 381 129 43	378 18 6 3	405
15	4681 1057 217 151	300 60 12 10	382
16	21845 13107 4369 3855 1285 771 257	1024 512 256 128 64 32 16	2032
18	87381 37449 29127 13797 12483 9709 4599 4161 3591 1971 1533 1387 1197 657 513 399 219 189 171 133 57 27 19	2592 1296 864 432 432 432 144 144 108 72 48 72 36 24 18 12 8 6 6 6 2 1 1	6756

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

IV. SIMULATIONS AND RESULTS

Simulations are carried out to find out the lengths of the non-maximal length sequences corresponding to polynomials of degree 6 to 20. All the polynomials of degrees 6 to 20 listed in [17] were considered in the simulation study. The polynomials were represented in octal notation. The octal string of each polynomial is parsed into individual octal digits, then each digit is converted to a binary number. The binary vector $\boldsymbol{h} = (h_0, h_1, \ldots, h_{n-1}, h_n)$ thus obtained is used to decide the feedback tap connections as described in section II.

Customized Matlab programs are developed for converting octal notation to feedback taps and then generating the binary linear feedback shift register (LFSR) sequences recursively. The recursive loop is continued to get a sequence $\boldsymbol{a}$ of $3.25N$ binary digits, accounting for more than 4 - 8 cycles of non-maximal length sequence depending the actual period of the sequence. The value of 3.25 is not mandatory, but is used for the unambiguous computation of autocorrelation peaks and subsequently the sequence period.

The cyclic correlation of the sequence is computed and a peak detection algorithm is applied to find out the correlation peaks, the sample count between the peaks is taken as the repetition period of the sequence. The measured periods $\hat{L}$, thus obtained for different polynomials in octal notation are listed in the third column of Table IV. For this work, in total around 20 customized functions in Matlab were developed for the polynomial representation, sequence generation, period computation and displaying of the results. All these functions are called in main program i.e. *PeriodityofNMLSequences.m*.

TABLE IV. POLYNOMIALS [TAPS] & PERIODS MEASURED OF NONMAXMIAL LENGTH SEQUENCES FOR DEGREE 6 TO 10

Degree	Polynomial Octal [Taps]	Period $\hat{L}$
6	127 [6 4 2 1 0]	21
	111 [6 3 0]	9
	165 [6 5 4 2 0]	21
8	567 [8 6 5 4 2 1 0]	85
	763 [8 7 6 5 4 1 0]	51
	675 [8 7 5 4 3 2 0]	85
	727 [8 7 6 4 2 1 0]	17
	613 [8 7 3 1 0]	85
	433 [8 4 3 1 0]	51
	477 [8 5 4 3 2 1 0]	85
	735 [8 7 6 4 3 2 0]	85
	637 [8 7 4 3 2 1 0]	51
	573 [8 6 5 4 3 1 0]	85
	643 [8 7 5 1 0]	85
	661 [8 7 5 4 0]	51
	771 [8 7 6 5 4 3 0]	85
	471 [8 5 4 3 0]	17
9	1231 [9 7 4 3 0]	73
	1027 [9 4 2 1 0]	73
	1401 [9 8 0]	73
	1511 [9 8 6 3 0]	73
	1145 [9 6 5 2 0]	73
	1641 [9 8 7 5 0]	73
	1003 [9 1 0]	73
	1113 [9 6 3 1 0]	73
10	2017 [10 3 2 1 0]	341
	2257 [10 7 5 3 2 1 0]	341
	2065 [10 5 4 2 0]	93
	2653 [10 8 7 5 3 1 0]	341
	3753 [10 9 8 7 6 5 3 1 0]	341
	3573 [10 9 8 6 5 4 3 1 0]	341
	3043 [10 9 5 1 0]	33
	2107 [10 6 2 1 0]	341
	3061 [10 9 5 4 0]	341
	2547 [10 8 6 5 2 1 0]	341
	3453 [10 9 8 5 3 1 0]	93
	3121 [10 9 6 4 0]	341
	2701 [10 8 7 6 0]	341
	2437 [10 8 4 3 2 1 0]	341
	2413 [10 8 3 1 0]	93
	2311 [10 7 6 3 0]	341
	3777 [10 9 8 7 6 5 4 3 2 1 0]	11
	3607 [10 9 8 7 2 1 0]	341
	2355 [10 7 6 5 3 2 0]	341
	3315 [10 9 7 6 3 2 0]	341
	3601 [10 9 8 7 0]	341
	3651 [10 9 8 7 5 3 0]	341
	2541 [10 8 6 5 0]	93
	3255 [10 9 7 5 3 2 0]	341
	3277 [10 9 7 5 4 3 2 1 0]	341
	3367 [10 9 7 6 5 4 2 1 0]	341
	3421 [10 9 8 4 0]	341
	2143 [10 6 5 1 0]	341
	3465 [10 9 8 5 4 2 0]	341
	3247 [10 9 7 5 2 1 0]	93
	2123 [10 6 4 1 0]	341
	2035 [10 4 3 2 0]	341
	3705 [10 9 8 7 6 2 0]	341
	3205 [10 9 7 2 0]	93
	2231 [10 7 4 3 0]	341
	3777 [10 9 8 7 6 5 4 3 2 1 0]	11
	3417 [10 9 8 3 2 1 0]	341
	2671 [10 8 7 5 4 3 0]	341
	2251 [10 7 5 3 0]	33
	2633 [10 8 7 4 3 1 0]	341

In addition to the above functions, 10 more Matlab programs are developed to compute the number of irreducible polynomials and the number of primitive polynomials through Möbius μ-function and Euler φ-function respectively. The results are used to populate the Tables I and II.

In the simulations study a total of 9840 (i.e. sum of values in the fourth column of Table III) sequences are generated, the measured periods from simulations are compared to the theoretical periods computed analytically using (3) and (4). Both the values are exactly same for all the 9840 sequences generated. To get an idea about the distribution of 1s and 0s visually, sample binary NML sequences ***a1*** through ***a8*** of degree 6 (period: 21) and degree 8 (period: 17, 51 and 85) along with the associated polynomials in octal form are displayed in Table V.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 5 Issue 05, May-2016

TABLE V. SAMPLE NONMAXMIAL LENGTH SEQUENCES

n=6 & L= 21	***Polynomial1= 127 (Octal)*** ***a1***=11111001110001000110 ***Polynomial2= 165 (Octal)*** ***a2***=11111011000100011100
n=8 & L= 17	***Polynomial1= 727 (Octal)*** ***a1***=11111111011000110 ***Polynomial2= 471 (Octal)*** ***a2***=11111111000101000
n=8 & L= 51	***Polynomial1= 763 (Octal)*** ***a1***=11111111011101010011100100100111111000110010111010 ***Polynomial1= 433 (Octal)*** ***a2***=11111111000010011100100010010100010110111000100000010 ***Polynomial1= 637 (Octal)*** ***a3***=11111111010111010011000111111001001001110010101011110 ***Polynomial1= 661 (Octal)*** ***a4***=11111111010000100011101101000101001000100111001010000
n=8 & L= 85	***Polynomial1= 567 (Octal)*** ***a1***=11111111001000110110100111001010000100010000011000011100000100111100110101001100100110 ***Polynomial2= 675 (Octal)*** ***a2***=11111111010001110101010110000101100110010000011011011100000010010110100000000011100100 ***Polynomial3= 613 (Octal)*** ***a3***=11111111010100100100011101011101111100010001001010000011000101101111011001111110010 ***Polynomial4= 477 (Octal)*** ***a4***=11111111000101100111100000101110100001010100110111101101100001000110111011010111110 ***Polynomial5= 735 (Octal)*** ***a5***=11111111011001001100101011001111001000001110001100000010001000010100111001011011000100 ***Polynomial6= 573 (Octal)*** ***a6***=11111111001001110000000101101001000000011101110110000010011001101000011010101011100010 ***Polynomial7= 643 (Octal)*** ***a7***=11111111010011111100111011110110100001100000110100100010001111101110101110001001001010 ***Polynomial8= 771 (Octal)*** ***a8***=11111111011111010011011101110001000011011011101100101010000101110100000111100110100

Matlab programs are also developed to display the results in ASCII string notation in compact form useful to populate the Table IV and V.

V. CONLUSIONS AND FUTURE WORK

The main focus of this work is the investigation of periodicity of the non-maximal length sequences generated by linear feedback shift registers. The paper discussed the mathematical structure associated with LFSR sequence generator. The number of primitive and non-primitive irreducible polynomials are computed analytically for the degrees 3 to 20. Simulations are carried out to generate a total of 9840 NML sequences corresponding to polynomials of degree 3 to 20. The period of each simulated sequence is computed to verify the analytical results. The repetition periods of all the simulated sequences are found to be exactly same as those obtained analytically. Sample NML sequences are also given.

The author conjectures that several applications other than communications might benefit from non-maximal length sequences. Some of such applications could be the sound synthesizers. Work is in progress by the author towards such an investigation.

REFERENCES

[1] Raymond L. Pickholtz et. al., "Theory of Spread-Spectrum Communications-A Tutorial" IEEE trans.Communications, Vol.-30, No. 5, May 1982 , pp. 885-884.

[2] Merrill I. Skolnik, "Introduction To Radar Systems", Chapter 11, Second Edition, McGraw-Hill, 1981.

[3] Peter Alfke, " Efficient shift registers, LFSR counters and Long Pseudo Random Sequences", Xlink Application Note, xapp052, July 7,1996 (Version 1.1)

[4] Xiang, N., "Using M-sequences for Determining the Impulse Responses of LTI-Systems," Signal Processing 28, , 1992, pp.139-152.

[5] W Chu. Impulse response and reverberation-decay measurements made by using a periodic pseudo random sequence,1977, pp.135-137

[6] D.D.Rife, "Modulation Transfer Function Measurement with Maximal Length Sequence," J. Audio Eng. Soc., Vol.40, Oct 1992, pp.779-790.

[7] D.D.Rife and J.Vanderkooy, "Transfer Function Measurement with Maximal Length Sequence," J. Audio Eng. Soc., Vol.37, June 1989, pp.419-443.

[8] J.Borish and J.B.Angell, "An efficient algorithm for Measuring the Impulse Response using Pseudo Noise", J. Audio Eng. Soc., Vol.31, July/Aug 1983, pp.478-488

[9] Nitin Yogi and Vishwani D. Agrawal, "Sequential Circuit BIST Synthesis using Spectrum and Noise from ATPG Patterns", Proc. 17th IEEE Asian Test Symp., Nov. 24-27, 2008, pp.69-74.

[10] Nitin Yogi and Vishwani D. Agrawal, "Application of Signal and Noise Theory to Digital VLSI Testing", 28th IEEE VLSI Test Symposium, April 2010, California, pp.215-220.

[11] R. Lisanke, F. Brglez, A. J. Degeus, , and D. Gregory, "Testability-Driven Random Test-Pattern Generation," IEEE Trans. on Computer-Aided Design, vol. 6, no. 6, Nov. 1987, pp. 1082–1087.

[12] John G.Proakis, "Digital Communications", McGraw-Hill, 1983.

[13] William Stallings, " Cryptography and Network Security: Principles and Practice, " Fifth Edition, Chapter 7, Prentice Hall, 2011.

[14] -, "Programmabe Tone/Noise generator: SN76496", Data Sheet, Texas Instruments, Jan 1989, pp.4-37 to 4-44.

[15] Solomon W.Golomb, "Shift Register Sequences", Holden-Day Inc., 1967.

[16] F. J. MacWilliams and N. J. A. Sloane, " Pseudo-Random Sequences And Arrays", Proc. IEEE,Vol.64, Dec 1976, pp.1715-1729.

W. Wesley Peterson, "Error Correcting Codes", M.I.T Press, 1965.