Available online at www.elixirpublishers.com (Elixir International Journal)

Electrical Engineering

Elixir Elec. Engg. 85 (2015) 34525-34527

ISSN: 2229-712X

FPGA Implementation of NO-Kumar Pseudo Random Sequences

Dundi Ajay, K.L.Sudha and A.Rajagopal
Department of ECE, DSCE, Bengaluru, India.

ARTICLE INFO

Article history:
Received: 28 June 2015;
Received in revised form:
1 August 2015;
Accepted: 19 August 2015;

Keywords
NO-Kumar sequences,
Trace function,
Odd correlation,
Even correlation,
Nexys-4 FPGA.

ABSTRACT

Binary pseudo random noise sequences are sequences of 1's and 0's having properties which make them appear to be noise-like but yet are deterministic. The NO-Kumar sequences were discovered by Jong-Seon No and P.V.Kumar and are known to have optimal correlation properties and a large linear span. The families of NO sequences are periodic with period = 2^n-1 where 'n' is an even integer and contain within them a GMW sequence and also small set of Kasami sequences as special case. In this paper we investigate the properties of these sequences such as balance, run and even correlation properties. Odd correlation properties of these sequences which are not described in the NO-Kumar paper are also highlighted. The sequences are first simulated in MATLAB and then implemented by writing a Verilog code on the Nexys 4 FPGA board.

Introduction

In spread spectrum multiple access communication systems it is desirable to have signals that have either or both of the following conditions met, (a) the signal should be easy to distinguish with a time shifted replica of itself, (b) signals in the set should be easy to distinguish from other time shifted signals in the set. These signals have been studied for the last 60 years and their generation methods and properties have been extensively studied. But certain applications like spread spectrum systems require that these pseudo random signals have good odd correlation properties along with even correlation properties, while Code Division Multiple Access (CDMA) systems require these signals to have low cross correlation. Signals which are used in anti-jamming and cryptographic applications should also have the additional property of having a large linear span. Signals based on linear feedback shift register like m-sequences, Gold and Kasami sequences have good auto-correlation properties but the drawback is that they have a small linear span. Pseudo random signal generators function similar to an oscillator in that they do not require an input to generate the output. Once the initial conditions or the state of the shift register are known the next state and the output is generated by the feedback connections. The length of the shift register for a given length of the pseudo random signal N is given by m = ceil($\log_2$N). The pseudo random signals employed in a number of applications are usually periodic as periodic signals are simpler to implement.

The family of NO-Kumar [1] sequences are periodic with N = 2^n– 1, where n = 2*m is an even integer. There are 2^m sequences within the family and the maximum over all nontrivial auto- and cross-correlation values equals 2^m +l. Each family contains a Gordon-Mills-Welch (GMW) sequence, and the families of sequences include the families of Kasami sequences (small set) as a special case. The linear span of these sequences varies within a family but is never less than the linear span of the GMW sequence contained within the family.

The rest of the paper is organized as follows: section II introduces NO-Kumar sequences and their shift register structure, section III contains the simulation results, section IV shows the FPGA implementation results with section V concluding the paper.

NO-Kumar Sequences

Let n, n > 0 be even, set N= 2^n -1, m = n/2, and T= 2^m+1. Then a family of NO-Kumar sequences is a collection of 2^m binary {0,l} sequences given by:

$S = \{s_i(t) \mid 0 \le t \le N-1,\ 1 \le i \le 2^m\}$, where

$$s_i(t) = tr_1^{m}\{[tr_m^{n}(\alpha^{2t}) + \gamma_i \alpha^{Tt}]^r\} \qquad \textbf{- (1)}$$

In Eq. (1) tr_m^n denotes the trace function [2,3] which is a mapping from Galois field GF(2^n) to GF(2^m) according to the rule

$$tr_m^{n}(x) = \sum_{j=0}^{\left(\frac{n}{m}\right)-1} x^{2^{j*m}} \qquad \textbf{- (2)}$$

In Eq. (1) 'α' is a primitive element of GF(2^n), the integer 'r' , 1 ≤ r ≤ 2^m-1, satisfies gcd(r,2^m-1) =1, and the elements γ_i range over all of GF(2^m) taking on each value once as 'i' ranges between 1 and 2^m. If the value of 'r' =1 then (1) gives the small set of Kasami sequences.

For implementation on a hardware platform like FPGA we slightly modify equation (1) by using the property of trace transform and replacing γ_i with α^{Tz} where,1 ≤ i ≤ 2^m then 0≤ z ≤ 2^m-2. The equation is as shown below

$$s_z(t) = tr_1^{m}\{[tr_m^{n}(\alpha^{t}) + \alpha^{2^{(m-1)}*T(t+z)}]^r\} \qquad \textbf{- (3)}$$

The structure shown in figure 1 of NO-Kumar sequences implemented in this paper is for n=6, m=3 and the primitive polynomial considered over GF(2) of degree 6 is f(x) =x^6 +x^5+ x^2 + x +1.

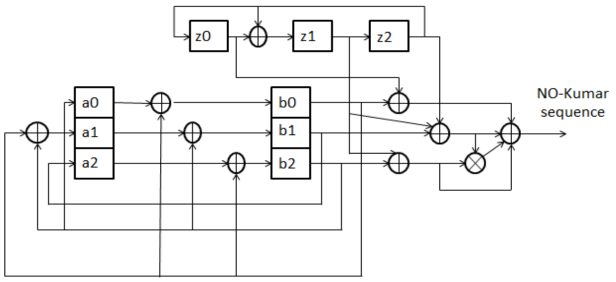

Figure 1. Shift register structure of NO-Kumar sequences of length 63 bits

Tele:
E-mail addresses: dundi.ajay@gmail.com

In the above figure ‘β’ = α^9 and is the primitive element of the polynomial x^3 + x +1 and the value of ‘r’ considered to generate the sequences is 3. The initial value of the shift registers ‘a’ and ‘b’ was kept fixed and the value of the shift register ‘z’ was changed thereby obtaining different sequences. The number of different sequences is given by the expression [φ(2^m-1)/m * φ(2^n-1)/n] where ‘φ’ indicates Euler’s totient function. The next section describes the properties of these sequences along with their results.

Simulation results

The various properties of a pseudo random sequence that are generally studied for use in spread spectrum communication are the balance property which indicates the number of 1’s to the number of 0’s, runs property- indicating the continuous runs of 1’s and 0’s and even and odd correlation properties.

The results of the balance property indicated that the difference between number of 0’s to 1’s was in the range {-1, -9, 7}.

Of all the “runs” of the sequence (i.e. runs consisting of 1’s and runs consisting of 0’s), the runs property states that ½ of runs are of length 1, ¼ of runs are of length 2, 1/8 of runs are of length 3 and so on. The result of NO-Kumar sequences for the input in the shift register z=[1 1 0] and z= [1 0 1] are shown in table 1.

Table 1. Runs test

No. of runs z= [1 1 0]	No. of runs z= [1 0 1]	Run length
10	22	1
9	9	2
8	3	3
0	1	4
1	2	5
1	0	6

Testing the runs property for all the sequences of length 63 bits indicated that they do not satisfy the property like the m-sequences.

The correlation property is of two types [4]: even or periodic correlation when there is no bit flip that occurs during transmission and odd or aperiodic correlation whenever a bit flip happens. The even correlation for a sequence ‘*a*’ consisting of -1’s and +1’s is defined as

$$\mathrm{ACF}_{\mathrm{even}}\,(\tau) = \textstyle\sum_{i=0}^{N-1} a_i\, a_{i+\tau} \qquad \text{- (4)}$$

$$\mathrm{CCF}_{\mathrm{even}}\,(\tau) = \textstyle\sum_{i=0}^{N-1} a_i\, b_{i+\tau}$$

ACF indicates auto-correlation whereas CCF denotes cross-correlation between sequences ‘a’ and ‘b’ and τ and N indicate the delay and length of the sequences respectively. The even correlation side-lobes are 3-valued taking the values in the set {-1, -9, 7) as shown in the figure below.

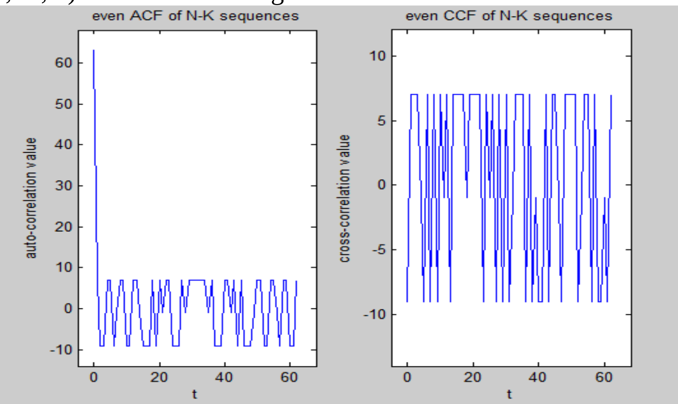

Figure 2. Even correlation of NO-Kumar sequences of length 63 bits

Odd or aperiodic correlation is defined as follows

$$\mathrm{ACF}_{\mathrm{odd}}\,(\tau) = \textstyle\sum_{i=0}^{N-\tau-1} a_i a_{i+\tau} - \sum_{i=N-\tau}^{N-1} a_i\, a_{i+\tau} \qquad \text{- (5)}$$

$$\mathrm{CCF}_{\mathrm{odd}}\,(\tau) = \textstyle\sum_{i=0}^{N-\tau-1} a_i b_{i+\tau} - \sum_{i=N-\tau}^{N-1} a_i\, b_{i+\tau}$$

Figure 3 shows the odd correlation side-lobes for the same two sequences of and unlike even correlation the side-lobes are not bounded and appear to be of random nature.

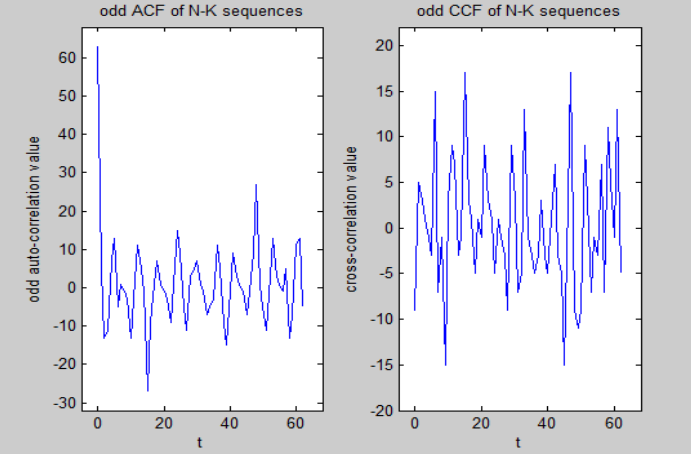

Figure 3. Odd correlation of NO-Kumar sequences of length 63 bits

The Welch bound [5] which gives the minimum of the maximum correlation achievable is given by the expression, Welch bound = n*sqrt{(M-1)/(Mn-1)} where ‘n’ is the length of the sequence and ‘M’ is the size of the family of sequences which are 63 and 12 respectively in our work. The correlation side-lobes of the NO-Kumar sequences shown in figure 2 and figure 3 are compared against the Welch bound in the following table.

Table 2. Welch bound comparison

Welch bound (dB)	Even ACF (dB)	Odd ACF (dB)	Even CCF (dB)	Odd CCF (dB)
-18.365	-16.90	-7.36	-16.90	-11.37

From the table we can conclude that although the even correlation is good the odd correlation side-lobes could degrade the performance of the system.

The NO-Kumar sequences when it comes to the linear span have the largest possible value, that is the linear span ≥ m*2^{m-1}compared to m-sequences, Gold, Kasami and bent sequences [6,7].

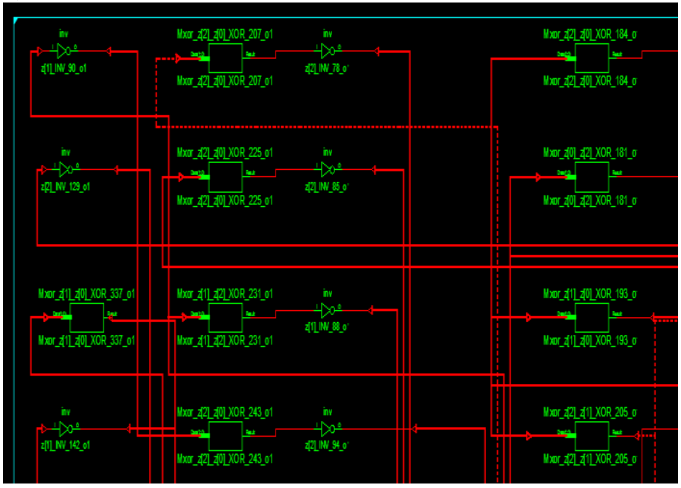

Figure 4. Part of an RTL schematic of NO-Kumar sequences

FPGA Implementation Results

The generation of sequence is implemented on the Nexys 4 Artix 7 FPGA**[8]**, with the code being written in Verilog. The Nexys4 board is a complete, ready-to-use digital circuit development platform based on the latest Artix-7™ Field Programmable Gate Array (FPGA) from Xilinx. With its large, high-capacity FPGA (Xilinx part number XC7A100T-

1CSG324C), generous external memories, and collection of USB, Ethernet, and other ports, the Nexys4 can host designs ranging from introductory combinational circuits to powerful embedded processors.

The Register Transfer Logic (RTL) schematic of the NO-Kumar sequence generation is as shown in figure 4 and the simulation results for initial conditions in the shift registers ‘a’ =[1 0 0], ‘b’ =[0 0 0] and ‘z’ =[0 0 0] is shown in figure 5.

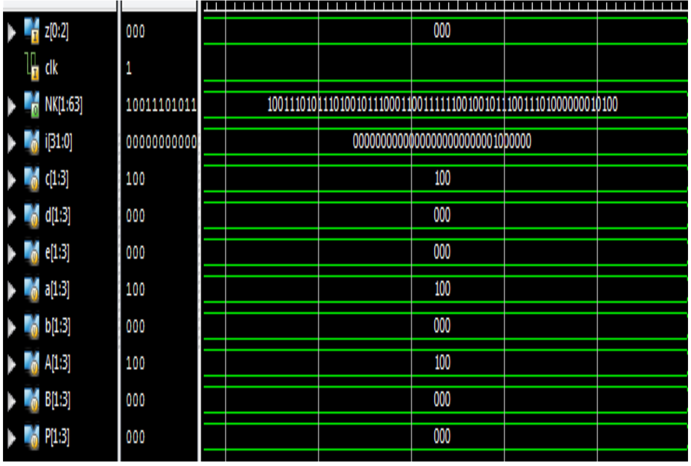
z[0:2] 000 000
clk 1
NK[1:63] 10011101011 1001110101110100101110001100111111100100101110011101000000010100
i[31:0] 00000000000 00000000000000000000000001000000
c[1:3] 100 100
d[1:3] 000 000
e[1:3] 000 000
a[1:3] 100 100
b[1:3] 000 000
A[1:3] 100 100
B[1:3] 000 000
P[1:3] 000 000

Figure 5. Simulation results using ModelSim

Table 3. Device utilization summary

Logic Utilization	**Used**	**Available**	**Utilization**
No. of slice LUT’s	35	63400	0%
No. of fully used LUT-FF pairs	0	35	0%
No. of bonded IOB’s	67	210	31%
No. of BUFG/BUFGCNTRL	1	32	3%

Conclusion

Sequences with low correlation are widely used in wireless communications for distinguishing multiple users or channels with low mutual interference. In addition, a large linear span also provides a major advantage by making the information less predictable and thereby increasing the security. The NO-Kumar sequences described here may not have the ideal properties required for say CDMA applications as seen with the results of the runs test and the aperiodic correlation results but their large linear span does make them suitable for cryptographic applications as it becomes difficult for an eavesdropper to predict the sequence. The FPGA implementation results indicate that the generation of these sequences is not complex. In future these sequences could be used as one of the possible encryption codes for the P(Y) codes of GPS systems.

Acknowledgment

This work was supported by ISRO RESPOND programme [grant no. ISRO/RES/3/651/2013-14]. The authors would also like to thank the following people, Sruthi, Harsha, Noopur and Lavanya for their support during the work.

References

[1] Jong-Seon No and P. Vijay Kumar, *“A New Family of Binary Pseudorandom Sequences Having Optimal Periodic Correlation Properties and Large Linear Span”,* IEEE Trans. Inform. Theory, vol. 35, no. 2, March 1989.

[2] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Spectrum Communications*, vol. I. Rockville, MD: Computer Science Press, 1985.

[3] Mc Eliece, Robert J, *Finite Fields,*1st Edition,Kluwer academic publishers, 2003.

[4] D. V. Sarwarte and M. B. Pursley, "*Crosscorrelation properties of pseudorandom and related sequences*," Proc. IEEE, vol. 68, no. 5, pp. 593-620, May 1980.

[5] L. R. Welch, "*Lower bounds on the maximum cross correlation of signals*," IEEE Trans. Inform. Theory, vol. IT-20, no. 3, pp.397-399, May 1974.

[6] R. Gold, "Optimal binary sequences for spread spectrum multi-plexing," IEEE Trans. Inform. Theory, vol. IT-13, no. 5, pp.619-621, Oct. 1967.

[7] J. D. Olsen, R. A. Scholtz, and L. R. Welch, "Bent-function sequences," IEEE Trans. Inform. Theory, vol. IT-28, no. 6, pp. 858-864, Nov. 1982.

[8] http://www.digilentinc.com/Products/Detail.cfm?Prod=NEXYS4.