Binary Sequences having Good Correlation and Large Linear Complexity Properties for Satellite Navigation Applications

Dileep Dharmappa, Mahalinga V Mandi, S. Ramesh

Abstract: ***LFSR based binary sequences are known to have good correlation and better balance property and hence they are used in Satellite Navigation Applications as signature sequences. However, due to the code length requirements of length being multiple of on-board fundamental frequency 10.23MHz in GNSS systems, often the LFSR based codes have to be truncated (like 10230 bits). Due to the truncation the correlation property and the balance property gets degraded. Apart from the correlation and balance properties of the binary sequences the linear complexity property also plays an important role for GNSS applications where in users need to be protected against unintended or unauthorized access like commercial applications or military applications. In this work the balance property, even correlation, odd correlation and linear complexity property of the state of the art binary sequences of length 10230 bits being used for one of the GNSS system namely Galileo E5b-I primary sequences of length 10230 bits are evaluated. A method for generation of binary sequences having properties better than Galileo E5b-I primary sequences are presented. Binary sequences generated from the proposed method is analyzed for balance, linear complexity and correlation properties. It is found that the proposed sequences have better balance, correlation properties and high linear complexity. Due to the high linear complexity property, the proposed sequences provide inherent security for the system against spoofing and hence make the GNSS system secure.***

Keywords: ***Even Correlation, Odd Correlation, Linear Complexity, Chaotic Map, Binary Sequences, CDMA, GNSS.***

I. INTRODUCTION

Binary spreading sequences enable multiple services in Global Navigation Satellites Systems (GNSS) Systems. GNSS System namely Galileo is the European GNSS (GALILEO) which has completed its one year of the Initial Service during December 2017. The Galileo System is designed to provide better performance and accuracy for GNSS community than the similar systems such as, Global Positioning System (GPS) by US, Russians Global Navigation Satellite System (GLONASS) and Chinese BeiDou Navigation Satellite System (BEIDOU). The Initial services offered by Galileo include Open Service, Public Regulated Service (PRS) and Search and Rescue Service (SAR). Out of the four frequency bands being used by Galileo namely E5a, E5b, E6 and E1, the three bands E5a, E5b and E1 lie in the allocated spectrum for Aeronautical Radio Navigation Services (ARNS) towards providing dedicated safety critical applications for GNSS users.

The Galileo offers four types of services to GNSS community, namely Open Service (OS), Commercial Service (CS), Public Regulated Service (PRS) and Search and Rescue Service (SAR). In the frequency band E5b centered at 1207.14MHz, Galileo offers Open Service and Commercial Service using E5b-I Signal component (European GNSS Agency, Issue 1.3, December 2016). We present the primary spreading codes of length 10230 bits used for Galileo E5b-I are generated and their properties are analyzed.

Balance and correlation properties are important for open services, while for commercial services along with the above properties the linear complexity properties play an important role. Less linear complexity will lead to the detection of the CDMA code being used for communication in commercial applications. By detecting the CDMA code used in a commercial application there exists a possibility of spoofing which can lead to misleading information and is not easy to detect, hence binary sequences with high linear complexity finds applications in commercial GNSS applications.

Novelty of this work lies in the fact that the problem of conversion of real valued chaotic binary sequences is addressed. A method for conversion of binary sequences is provided in which the generated binary sequences retains the properties of the chaotic sequences. The generated binary sequences using the proposed method are found to be nonlinear and hence possess large linear complexity property. The generated sequences retain the odd and even correlation properties of the chaotic real valued sequences and hence the proposed sequences have better correlation properties both the odd correlation and even correlation properties as compared with LFSR based binary sequences. The results presented in this work are evident to prove the fact that the proposed method is novel in retaining the real valued chaotic sequences properties in the generated binary sequences.

Balance Property, Correlation Properties and Linear Complexity Property

Important properties for binary sequences used in CDMA namely correlation property, balance property and Linear Complexity property are defined in this section.

Manuscript received January 25, 2019.

Dileep Dharmappa*, Research Scholar, Department of Electronics and Communication Engineering (ECE), Sri Siddhartha Academy of Higher Education (SSAHE), Agalakote, Tumkur, Karnataka, India.
Navigation Systems Area, ISTRAC, ISRO, Bangalore, Karnataka,India.
Mahalinga V Mandi, Department of Electronics and Communication Engineering (ECE), Dr.Ambedkar Institute of Technology, Near Jnana Bharathi, Bengaluru, Karnataka, India.
S. Ramesh, Department of Electronics and Communication Engineering (ECE), Dr.Ambedkar Institute of Technology, Near Jnana Bharathi, Bengaluru, Karnataka, India.

These properties serve as the performance metrics of the codes used in GNSS.

Odd and Even Correlation Functions

The Aperiodic correlation function (Sarwate and Pursley 1980) for two binary sequences x and y of length N bits is defined as

$$C_{x,y}(l) = \begin{cases} \sum_{j=0}^{N-1-l} x_j y_{j+l}^*, & 0 \le l \le N-1 \\ \sum_{j=0}^{N-1+l} x_{j-l} y_j^*, & 1-N \le l \le 0 \\ 0, & |l| \ge N. \end{cases} \quad (1)$$

$l$is the number of locations by which one sequence say y is shifted with respect to the other sequence x. N is the length of sequence.

Then the Even Cross Correlation (even CCR) function of two sequences x and y of length N symbols is defined (Sarwate and Pursley 1980) as,

$$\theta_{x,y}(l) = C_{x,y}(l) + C_{x,y}(l-N) \quad (2)$$

Here x and y are two different sequences, is the length of the sequences and N is the number of shifts.

Even Auto Correlation (even ACR) function of a sequences x of length N symbols is defined as,

$$\theta_{x,x}(l) = C_{x,x}(l) + C_{x,x}(l-N) \quad (3)$$

Here x is the sequence, l is the length of the sequence and N is the number of shifts.

Also the Odd Cross Correlation (odd CCR) function of two sequences x and y of length N symbols is defined (Sarwate and Pursley 1980) as,

$$\hat{\theta}_{x,y}(l) = C_{x,y}(l) - C_{x,y}(l-N) \quad (4)$$

Here x and y are two different sequences, l is the length of the sequences and N is the number of shifts.

Odd Auto Correlation (odd ACR) function of a sequences x of length N symbols is defined as,

$$\hat{\theta}_{x,x}(l) = C_{x,x}(l) - C_{x,x}(l-N) \quad (5)$$

Here x is the sequence, l is the length of the sequence and N is the number of shifts.

Even cross correlation is the primary property responsible for identification of the Satellite among different satellites from GNSS Systems. The odd correlation function represents the output of the correlator when the data symbol or PRN code bit changes during the integration time due to Multipath, Interference etc(channel noise). Whereas the even correlation function represents the correlator output when data symbol does not change during the correlation integration interval. Any binary sequence derived from mathematical (analytic) formulae can only offer good even correlation performance (Stefan, Jose and Avila 2011).Hence researchers are interested in designing binary spreading sequences with better odd correlation for DS-CDMA based Systems from early 1990 onwards(Fukumasa et al. 1994;Zhu et al. 1999;Dudkov et al. 2005).

Linear Complexity Property

Definition: Linear complexity (Massey 1969) of a binary sequence of finite length is the length of the shortest LFSR that generates the same sequence. Berlekamp – Massey algorithm (Massey 1969) is an efficient algorithm for determining the linear complexityor linear span of binary sequence of finite length.

Balance Property

Definition: The occurrence of 0 and 1 in the binary sequence should be approximately the same. The number of ones equals the number of zeros plus one, since the state containing only zeros cannot occur.

The LFSR based sequences are known to possess perfect balance property. But due to truncation of bits the sequences will tend to lose the balance property. The balance property is very important for GNSS Systems for reception of navigation data. It is to be noted that to guarantee efficient spread spectrum communication, bit balancing property of spreading code is essential. The balanced code sequences will have zero dc components by definition. The perfect zero balance in the code at the transmitter end of GNSS Satellites will ensure that there is no carrier leakage in the local oscillator at the receiver end in GNSS receivers. Any carrier leakage at the receiver will effect on the data decoding part of the receiver. If the sequences are imbalanced at the transmitter this will be seen as a DC component at the receiver end in GNSS systems and this DC component has to be compensated by the receivers.

Correlation Property, Balance Property and Linear complexity property of Galileo E5b-I Sequences

The Galileo E5b-I code used in the open service signal which has improved navigation accuracy and repeat every 1ms period. The Galileo E5b-I Sequences are obtained by short cycling the LFSR for every count of 10230 chips by resetting with a specified initial state

Generation of Galileo E5b-I binary sequences

As provided by the latest Galileo ICD(European GNSS Agency, Issue 1.3, December 2016), updated during December 2016, the Galileo E5b-I primary ranging codes of length 10230 bits are LFSR based codes reset after 10230 bits. From ICD (European GNSS Agency, Issue 1.3, December 2016) it can be observed that the chip rate of Galileo E5b-I ranging code is1.023 MCps.

The polynomial used to generate the E5b-I signal is 112341 (octal) and 111222 (octal) of degree 14.

LFSR based sequences are most commonly used binary sequences for GNSS.

However for GNSS Signals, it is desirable to have binary sequences period to be multiple of on-board fundamental frequency (10.23MHz) i.e., multiple of 1023. Considering tenth multiple1023x10, we get 10230 bits as the required binary sequence length.

Due to the non-availability of 10230 bit LFSR sequences the binary sequences from LFSR are truncated/short cycled. For Galileo E5b-ISequences the 14 bit LFSR provides sequences of length (2^{14}-1) which is 16383 bits. The 6153 bits are discarded to obtain the 10230 bit binary Galileo E5b-I sequences.

A set of 50Galileo E5b-I binary sequences of length 10230 bits are generated from the LFSR method by selecting different initial values for LFSR and short cycling to 10230 bits. The initial values of LFSR are provided in Table 01. It is to be noted that, even though the information provided in Table-01 is available in the literature (European GNSS Agency, Issue 1.3, December 2016) this table is reproduced for the sake of completion.

Table 1: Shift register values for generation of Galileo E5b-I Sequences (European GNSS Agency, Issue 1.3, December, 2016).

E5B-I Code Number	Shift register Start Value(Octal)	E5B-I Code Number	Shift register Start Value(Octal)
1	7220	26	25664
2	26047	27	21403
3	252	28	32253
4	17166	29	2337
5	14161	30	30777
6	2540	31	27122
7	1537	32	22377
8	26023	33	36175
9	1725	34	33075
10	20637	35	33151
11	2364	36	13134
12	27731	37	7433
13	30640	38	10216
14	34174	39	35466
15	6464	40	2533
16	7676	41	5351
17	32231	42	30121
18	10353	43	14010
19	755	44	32576
20	26077	45	30326
21	11644	46	37433
22	11537	47	26022
23	35115	48	35770
24	20452	49	6670
25	34645	50	12017

To study the properties ofGalileo E5b-I Sequences, 50 binary spreading sequences of length 10230 bits were generated using MATLAB and investigation is carried out for even and odd correlation properties. The results of maximum off peak even ACR and maximum off peak Odd ACR values for Galileo E5b-I Sequences are tabulated in Table 02. The off peak even ACR was found to be multiple valued and no more three valued due to the truncation of6153bits. The histogram of off peak odd ACR for all the 50Galileo E5b-I binary sequences are as shown in Figure 1. From Table 02, it is observed that maximum even ACR for the set of 50 sequences of length 10230 bits is -28.74dB.

The off peak odd ACR was found to be multiple valued. The histogram of off peak odd ACR for all the 50Galileo E5b-I binary sequences are as shown in Figure 2. From Table 02, it is observed that maximum odd ACR for the set of 50 sequences of length 10230 bits is -28.51dB.

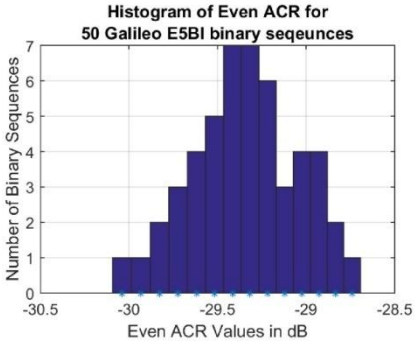

Figure 1: Histogram of maximum off peak even ACR for 50 Galileo E5b-I binary sequences

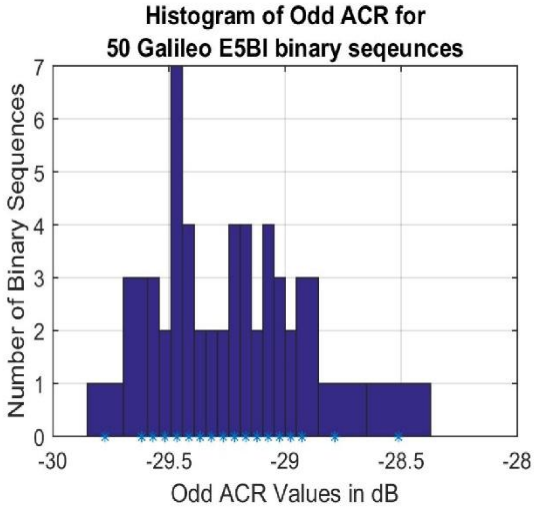

Figure 2: Histogram of maximum off peak odd ACR for 50 Galileo E5b-I binary sequences

Table 2: Off Peak Maximum even ACR and odd ACR for 50 Galileo E5b-I Sequences.

Sequence Number	Off Peak Maximum even ACR Value	Off Peak Maximum odd ACR Value	Sequence Number	Off Peak Maximum even ACR Value	Off Peak Maximum odd ACR Value
1	-29.316	-29.568	26	-29.416	-29.416
2	-29.023	-29.169	27	-28.928	-29.217
3	-29.619	-29.619	28	-29.723	-28.928
4	-29.723	-29.568	29	-29.619	-29.466
5	-29.316	-29.169	30	-29.023	-29.071
6	-29.416	-29.466	31	-29.120	-29.071
7	-29.827	-29.071	32	-29.217	-29.217
8	-29.416	-29.466	33	-29.517	-29.775
9	-29.316	-29.120	34	-29.517	-29.416
10	-30.040	-29.619	35	-28.740	-28.511
11	-29.517	-29.023	36	-29.217	-28.787
12	-29.416	-28.975	37	-29.416	-29.366
13	-29.023	-29.071	38	-29.416	-29.023
14	-29.217	-29.217	39	-29.217	-29.568
15	-29.619	-29.517	40	-29.517	-29.517
16	-29.723	-29.619	41	-29.316	-29.120
17	-29.217	-29.169	42	-29.120	-29.267
18	-29.316	-28.928	43	-28.928	-28.975
19	-29.416	-29.366	44	-29.517	-29.316
20	-28.833	-29.416	45	-29.023	-29.466
21	-29.619	-29.466	46	-29.316	-29.316
22	-29.316	-29.267	47	-28.928	-29.466
23	-29.120	-29.217	48	-29.217	-29.466
24	-29.827	-29.023	49	-28.928	-28.928
25	-29.933	-29.416	50	-28.833	-29.169

The Histogram results of all 1225 combinations of pairwise maximum even CCR for 50Galileo E5b-I binary sequences are as shown in Figure 3. From the histogram it can be observed that due to the effect of truncation, the results of cross correlation are not three valued and the maximum pairwise even cross correlation is -25.20dB.

The Histogram results of all 1225 combinations of pairwise maximum odd CCR for 50GalileoE5b-Ibinary sequences are as shown in Figure 4. The maximum pairwise odd cross correlation for a set of 50Galileo E5b-Ibinary sequences is found to be -25.04dB.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

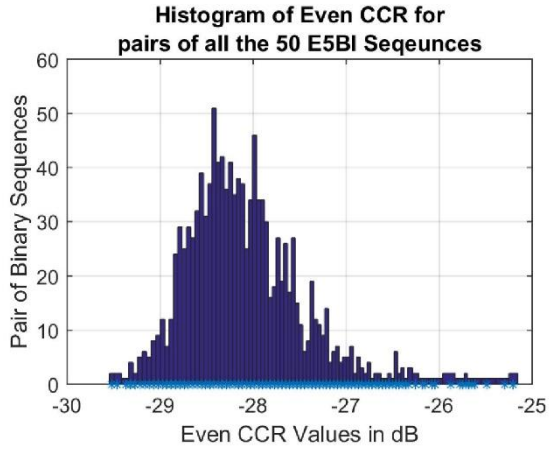

Figure 3: Histogram of maximum pairwise even CCR for 1225 pairs of 50 Galileo E5b-I binary sequences.

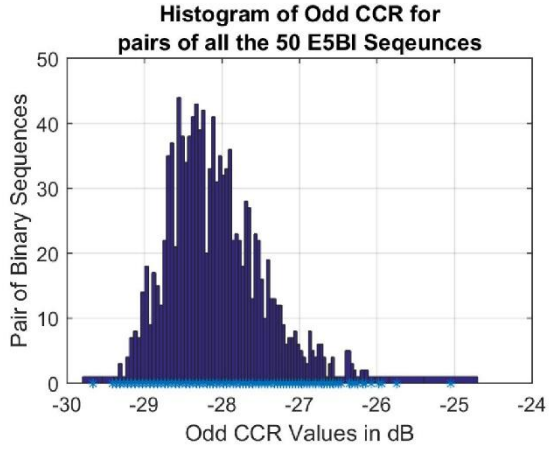

Figure 4: Histogram of maximum pairwise odd CCR for 1225 pairs of 50 Galileo E5b-I binary sequences

Proposed Method for generation of binary sequences of 10230 bits length

A method is proposed for generating binary sequences using chaotic function and is shown in Figure 5. In the proposed method, the most commonly used chaotic function namely Logistic Map (Heidari-Bateni et al. 1994; Ling et al. 2000; Mandi et al. 2010; Wang et al. 2017) is considered and is given by the following equation (Robert 1976)

$$S_{k+1} = BS_k(1 - S_k)(6)$$

where $S_k$is defined over real, 0<S<1, B is called bifurcation parameter or control parameter and 3.57<B< 4.

Discrete logistic map function iteratively generates a real valued infinite sequence $\{S_k\}$, k = 0,1,2,….., with S_0 in specified range, makes each S_k to lie in the same range. Each element S_k of sequence $\{S_k\}$ is first multiplied by a large integer E. The integer part of the result of multiplication is considered as Q_k and the fractional part is discarded. The large value of integer part Q_k is then reduced to small integer Y_k by performing modulo operation with smaller integer G. Integer Y_k is converted to binary sequenceP_k. In the proposed method it is necessary that G<E. The proposed method is governed by the equation (7).

$$Y_k = \lfloor (S_k) * E \rfloor mod(G)(7)$$

The binary sequences generated using the proposed method are investigated for auto correlation and cross correlation, balance property and linear complexity properties.

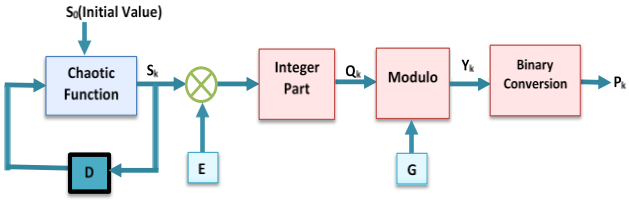

Figure 5: Proposed method for binary sequence generation of length 10230 bits from chaotic real sequences.

Properties of Binary Sequences of 10230 bits length generated from the proposed method

100 binary sequences of length 10230 bits were generated from the proposed method by selecting the initial values randomly and setting integer G=4 and E=32767. Set of 60 sequences with better correlation properties were selected by MATLAB simulations.

Correlation properties of Generated Binary sequences from the proposed method.

The generated sequences were investigated for odd auto correlation and even auto correlation properties. The results of maximum off peak even ACR and maximum off peak odd ACR for all the generated 60 sequences of length 10230 bits are provided in Table 03. The histogram of maximum off peak even ACR sequences is as shown in Figure 6. It is observed that the maximum off peak even ACR was found to be -29.02dB. The results of histogram of maximum off peak odd ACR for all 60sequences is provided in Figure 7. It is found that the maximum off peak odd ACR for a set of 60 binary sequences of 10230 bits is -29.02dB.

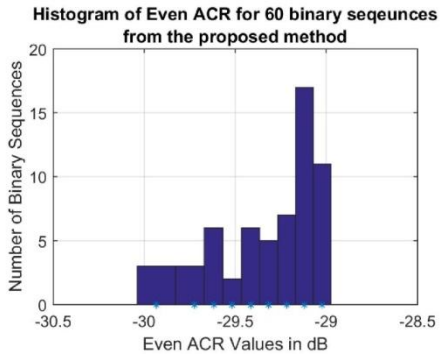

Figure 6: Histogram of maximum off peak even ACR for 60 proposed binary sequences.

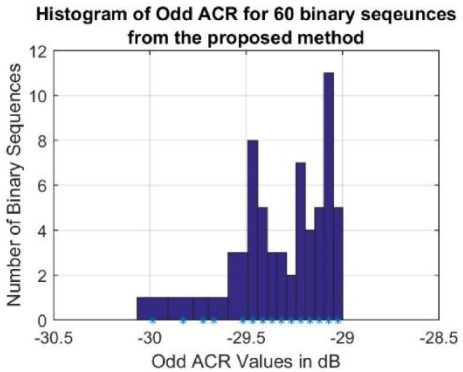

Figure 7: Histogram of maximum off peak odd ACR for 60 proposed Binary sequences

Table 3: Off Peak Maximum even ACR and maximum off peak maximum odd ACR for generated 60 binary sequences.

Sequence Number	Off Peak Maximum even ACR Value	Off Peak Maximum odd ACR Value	Sequence Number	Off Peak Maximum even ACR Value	Off Peak Maximum odd ACR Value
1	-29.120	-29.120	31	-29.316	-29.169
2	-29.023	-29.023	32	-29.023	-29.217
3	-29.316	-29.316	33	-29.619	-29.217
4	-29.416	-29.416	34	-29.120	-29.267
5	-29.217	-29.217	35	-29.217	-29.169
6	-29.517	-29.517	36	-29.217	-29.416
7	-29.023	-29.023	37	-29.316	-29.120
8	-29.416	-29.416	38	-29.120	-29.366
9	-29.723	-29.723	39	-29.120	-29.267
10	-29.120	-29.120	40	-29.120	-29.827
11	-29.217	-29.217	41	-29.619	-29.466
12	-29.120	-29.120	42	-29.120	-29.071
13	-29.120	-29.120	43	-29.933	-29.366
14	-29.416	-29.416	44	-29.120	-29.416
15	-29.217	-29.217	45	-29.316	-29.071
16	-29.120	-29.120	46	-29.619	-29.416
17	-29.023	-29.023	47	-29.933	-29.466
18	-29.217	-29.217	48	-29.120	-29.517
19	-29.723	-29.723	49	-29.120	-29.671
20	-29.023	-29.023	50	-29.023	-29.169
21	-29.416	-29.416	51	-29.316	-29.120
22	-29.217	-29.217	52	-29.619	-29.416
23	-29.023	-29.023	53	-29.619	-29.466
24	-29.023	-29.023	54	-29.517	-29.023
25	-29.120	-29.120	55	-29.023	-29.316
26	-29.120	-29.120	56	-29.723	-29.316
27	-29.120	-29.120	57	-29.023	-29.169
28	-29.023	-29.023	58	-29.120	-29.466
29	-29.619	-29.619	59	-29.933	-29.023
30	-29.416	-29.416	60	-29.416	-29.416

The Histogram results of all 1770combinations of pairwise maximum even CCR for a set of proposed 60 binary sequences are as shown in Figure 8. From the histogram it can be observed that the maximum pairwise even cross correlation is -25.71dB.

The Histogram results of all 1770combinations of pairwise maximum odd CCR for proposed set of 60 binary sequences are as shown in Figure 9. The maximum pairwise odd cross correlation for a set of 60 binary sequences of length 10230 bits are found to be -25.51dB.

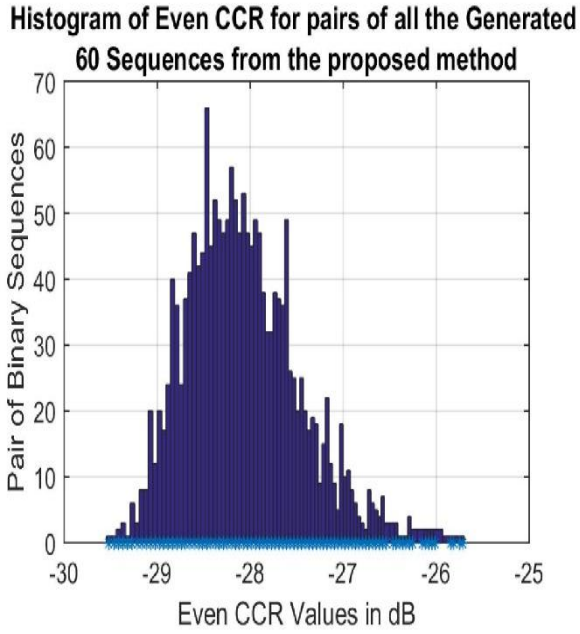

Figure 8: Histogram of maximum pairwise even CCR for 1770 pairs of 60 proposed binary sequences

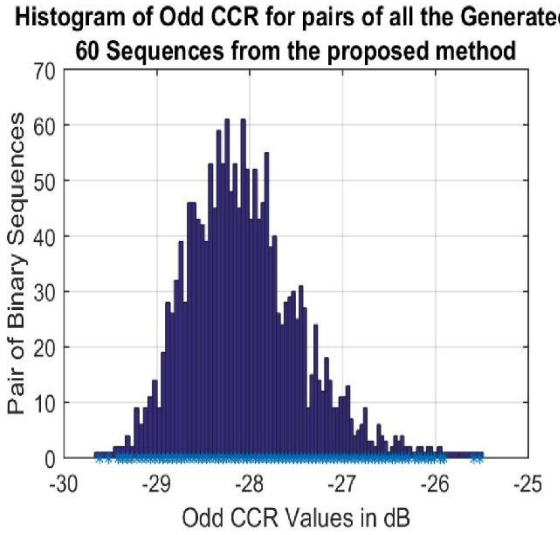

Figure 9: Histogram of maximum pairwise odd CCR for 1770 pairs of 60 proposed binary sequences

Linear complexity property of the generated sequences

The linear complexity property profile of the generated 60binary sequences of length 10230 bits were computed using Berleykamp- Massey Algorithm (Massey 1969). The Linear complexity profile is as shown in Figure 10. The blue line represents the expected linear complexity for ideal random sequences of length 10230 bits i.e., 5115. The red line represents the Linear Complexity of the proposed 60 binary sequences. From the Figure 10 it can be observed that the proposed binary sequences possess the near ideal linear complexity property. Table 04 provides the actual linear complexity of each proposed binary sequences and the initial value used for generating these binary sequences. It is clearly observed from Table 04 that the linear complexity for 10230 bits binary sequences proposed is 5115 ± 4.LC The LC value of the all 50Galileo E5b-I Sequences were found to be 28, this was expected due to the use of LFSR of 14 bits. As compared to LC value of 28 for Galileo E5b-I sequences, the LC for generated binary sequence of length 10230 bits is 5115 ± 4, hence these sequences provide better security to the GNSS Systems.

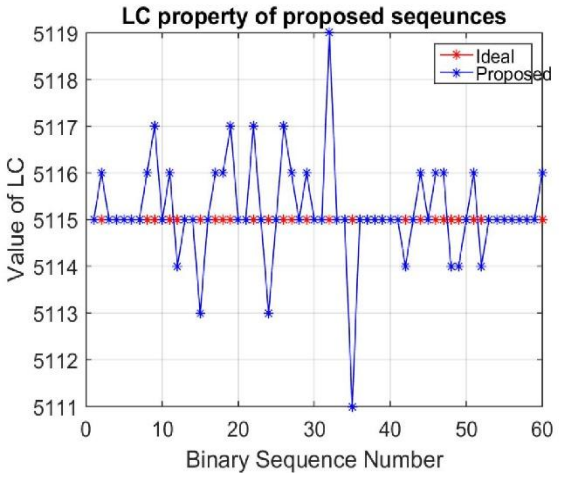

Figure 10: Linear Complexity Profile of Generated 60 Proposed Binary Sequences of length 10230 bits

Table 4: Initial values of the generated binary sequences using proposed method and Linear Complexity of 10230 bit sequences.

Sequence Number	Initial value	LC	Sequence Number	Initial value	LC
1	0.212541877	5115	31	0.306624283	5115
2	0.275616273	5116	32	0.485994169	5119
3	0.302827689	5115	33	0.116546433	5115
4	0.475244826	5115	34	0.989395941	5115
5	0.410956614	5115	35	0.815226955	5111
6	0.654511402	5115	36	0.9621145	5115
7	0.423519967	5115	37	0.794600969	5115
8	0.526577366	5116	38	0.333812096	5115
9	0.438615061	5117	39	0.608707125	5115
10	0.543978004	5115	40	0.279169156	5115
11	0.742764446	5116	41	0.258922021	5115
12	0.589866713	5114	42	0.494955348	5114
13	0.204700059	5115	43	0.61660699	5115
14	0.086807415	5115	44	0.068485006	5116
15	0.28460739	5113	45	0.739075846	5115
16	0.466677634	5115	46	0.634039138	5116
17	0.551158238	5116	47	0.845383405	5116
18	0.481239775	5116	48	0.435453883	5114
19	0.206890307	5117	49	0.193422061	5114
20	0.084117599	5115	50	0.713860412	5115
21	0.349169262	5115	51	0.247436989	5116
22	0.490344617	5117	52	0.480668344	5114
23	0.183406996	5115	53	0.948742953	5115
24	0.351953504	5113	54	0.37995636	5115
25	0.330252116	5115	55	0.198601429	5115
26	0.652046568	5117	56	0.6847719	5115
27	0.966134258	5116	57	0.937364032	5115
28	0.163150226	5115	58	0.000457892	5115
29	0.677527007	5116	59	0.872243032	5115
30	0.919070069	5115	60	0.082483194	5116

Balance Property

The balance property for the generated sequences and the Galileo E5B-I sequences are as shown in the Figure 11. From the figure11 it can be observed that the maximum imbalance in the proposed sequences is 48 bits for 10230 bit binary sequences. Thus the proposed sequences possess good balance properties.

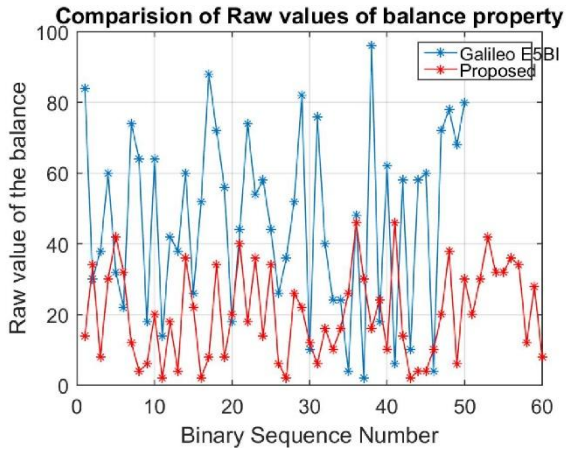

Figure 11: Balance of Proposed Binary Sequences as compared with Galileo E5BI Sequences

Comparison of Properties of Proposed Binary Sequences with Galileo E5b-I Sequences

The Table 05 compares the properties of the proposed binary sequences with Galileo E5b-I binary sequences. Following are the observations

1) The proposed binary sequences is having 0.28dB better even ACR and 0.51dB better odd ACR as compared to Galileo E5b-I binary sequences, hence these sequences will offer better performance during acquisition process for GNSS systems.
2) The proposed binary sequences is having 0.51dB better even CCR and 0.47 dB better odd CCR as compared to Galileo E5b-I binary sequences, hence these sequences will offer better performance during tracking process for GNSS systems.
3) The proposed binary sequences is having better balance of 48 bits as compared to 96 bits for Galileo E5b-I binary sequences. This will help GNSS Systems having less effect of imbalance as observed from Galileo E5b-I binary sequences.
4) The proposed binary sequences has high linear complexity of 5115±4 as compared to 28 for Galileo E5b-I binary sequences. This will ensure that sequences cannot be decoded easily and hence will provide inherent security to the GNSS system without encryption systems.
5) The proposed sequences are 60 in number as compared to 50 sequences of Galileo E5b-I binary sequences and hence the method is capable of generating more sequences required for GNSS systems.

Table 5: Comparison of Proposed Binary Sequences with Galileo E5b-I Sequences of length 10230 bit.

Sequences	Even ACR in dB	Odd ACR in dB	Even CCR in dB	Odd CCR in dB	LC	Balance in bits	Number of Sequences
Galileo E5b-I Sequences	-28.74	-28.51	-25.20	-25.04	28	96	50
Proposed Sequences	-29.023	-29.023	-25.71	-25.51	5115 ±4	48	60
Improvement	0.28	0.51	0.51	0.47	5084	20	10

II. CONCLUSION

In this work a method is proposed for generation of binary sequences which retain the properties of chaotic real valued sequences such as good odd correlation and good even correlation properties and non-linearity properties. Towards understanding the properties of binary sequence used in GNSS systems, the state-of-the-art binary sequences set of 50 sequences namely Galileo E5b-I binary sequences are generated. The odd correlation, even correlation, balance and the linear complexity properties are investigated. It is observed that even though Galileo E5b-I sequences are generated from the LFSR based method, the binary sequences are not balanced perfectly balanced. It is also observed that these sequences are optimized for both even and odd correlation properties.

The even and odd auto correlation properties of these sequences are excellent as compared to their cross correlation counterparts, or in other words these sequences are optimized for acquisition performance. It is also observed that the auto correlation and the cross correlation properties of Galileo E5b-I Sequences are multiple valued due to truncation.

Using the proposed method a set of 60 binary sequences are generated. It is observed that the proposed sequences as compared to the Galileo E5b-I Sequences are having better off peak even ACR of 0.28 dB, off peak odd ACR of 0.51 dB, pairwise even CCR of 0.51 dB and pairwise odd CCR of 0.47 dB, hence these sequences are having better margin during acquisition and tracking process of GNSS Signals. The proposed sequences linear complexity profile is near to ideal random sequences hence the use of these sequences in GNSS systems will require no cryptographic algorithms for providing services to commercial users where security of GNSS systems are of high concern. Also since these sequences will provide inherent security to the GNSS system, at the user receiver end need of cryptographic algorithms being implemented can be removed and the hardware can be of smaller size due to the removal of cryptographic measures and hence the proposed method is suitable for GNSS Applications.

REFERENCES

1. Dudkov Alexey, Valery P Ipatov (2005) Signature-interleaved DS CDMA controlling odd correlation peaks. IEEE 16th International Symposium on Personal, Indoor and Mobile Radio Communications. 4:2527-2530.
2. Fukumasa Hidenobu, Ryuji Kohno, Hideki Imai (1994) Design of pseudonoise sequences with good odd and even correlation properties for DS/CDMA. IEEE Journal on Selected Areas in Communications. 12(5):828-836.
3. Galileo Interface Control Document (2016) Galileo Open Service Signal In Space Interface Control Document OS SIS ICD 1.3. Publishing European GNSS Agency. https://www.gsc-europa.eu/system/files/galileo_documents/Galileo-OS-SIS-ICD.pdf Accessed 26 January 2018
4. Heidari-Bateni G, McGillem C D (1994) A Chaotic Direct-Sequence Spread-Spectrum Communication System. IEEE Transactions on Communications. 42(234): 1524-1527.
5. Ling Cong, Li Shaoqian (2000) Chaotic Spreading Sequences with Multiple Access Performance Better than Random Sequences. IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications. 47(3):394-397
6. Mahalinga V Mandi, K N HariBhat, R Murali (2010) Generation of Large Set of Binary Sequences derived from Chaotic Functions with Large Linear Complexity and Good Cross Correlation Properties. International Journal of Advanced Engineering and Applications (IJAEA) III:313-322.
7. Massey J L (1969) Shift Register Synthesis and BCH Decoding. IEEE Trans. on Information Theory. 15(1):122-127.
8. Robert M May (1976) Simple Mathematical Models with Very Complicated Dynamics. 261: 459–467.
9. Sarwate D V, Pursley M B (1980) Cross correlation Properties of Pseudorandom and Related Sequences. Proceedings of IEEE. 68(5):593-619
10. Wang D, Xue R, Sun Y (2017) A ranging code based on the improved Logistic map for future GNSS signals: code design and performance evaluation. J Wireless Com Network. 2017(1):57.
11. Zhu Y, T T Tjhung, H K Garg (1999) A new family of polyphase sequences for CDMA with good odd and even correlation properties. 2nd IEEE Workshop on Signal Processing Advances in Wireless Communications (Cat. No.99EX304).

AUTHOR BIOGRAPHIES

Dileep D completed M.Tech form Visvesvaraya Technological University (VTU) in 2009, He is working as Scientist/Engineer at ISTRAC-ISRO, Bangalore. He is currently pursuing PhD from Sri Siddhartha Academy of Higher Education (SSAHE). His areas of interest include Digital communication, Cryptography, Digital Signal Processing, Satellite Navigation Systems, PRN code design for GNSS systems, Ground segment for GNSS systems, Chaotic Maps and Binary Sequence design.

Mahalinga V Mandi completed his PhD from Dr M.G.R University, in 2013, His areas of interests include Digital Signal Processing, Digital Communication, Cryptography and Network Security, VLSI Design and Digital Circuits, Chaotic Maps, Binary Sequence design, GNSS.

Ramesh S completed B E, E&C Gulbarga University, M.Tech from form Visvesvaraya Technological University (VTU) and PhD from Dr M.G.R University, in 2013. He is currently working as Associate Professor at Department of ECE in Dr.Ambedkar Institute of Technology and has published about 30 papers in national and international national conferences and journals. His areas of interests include Cryptography, Digital Communication, Analog Communication, VLSI Design, VHDL coding and Digital Circuits, Chaotic Maps, Binary Sequence design.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication