Legendre and Polyphase Sidel'nikov Sequence for Applications in Space Communication

Cheruku Ravikumar, K. L. Sudha

Abstract— Pseudo Random Noise (PRN) codes are essential part in space communication. A pseudo random noise binary sequence is a semi-random sequence in the sense that it appears random within the sequence length, fulfilling the needs of randomness. The objective of the paper is to generate different types of PN sequences i.e. Legendre sequence, Weil sequence, Sidel'nikov sequence and polyphase Sidel'nikov sequence which are used for space communication applications and compare their randomness characteristics. Legendre sequences are generated based on the ON-THE-FLY code generation method. Weil sequence is obtained by performing EX-OR of the Legendre sequence and a circular shift of Legendre sequence. In this paper, the different types of PN sequences are used to construct the spread spectrum communication system with BPSK modulation.

Index Terms— Legendre sequence, Weil sequence, Sidel'nikov sequence, Finite field.

I. INTRODUCTION

Sequences with low correlation are widely used in wireless communications for acquiring the correct timing information well as distinguishing multiple users/channels with low mutual interference. In addition, a large number of distinct sequences are also required for supporting as many distinct users or channels as possible. **Pseudo Random Noise (PRN)** codes are essential element in space communication. A pseudo random noise binary sequence is a semi-random sequence in the sense that it appears random within the sequence length, fulfilling the needs of randomness, but the entire sequence repeats indefinitely. To a casual observer the sequence appears totally random, however to a user who is aware of the way the sequence is generated and all the properties are known, the sequence become deterministic. Because of their good auto correlation, two similar PN sequences can be easily be phase synchronized, even when one of them is corrupted. Noise-like wideband spread-spectrum signals are generated using PN sequence. In DS/SS (direct sequence spread spectrum), a PN spreading waveform is a time function of PN sequence and the time waveform generated from PN sequence also seems like random noise.

Direct sequence spread spectrum (DSSS) is a spread spectrum technique wherein the original data signal is multiplied with a pseudo random noise spreading code. DSSS significantly improves protection against interfering (or jamming) signals, which are narrowband and makes signal unnoticeable. It also provides security of transmission if the code is not known to the public. These reasons make DSSS very popular in military communication application.

Manuscript Received on July 20, 2014.

Cheruku Ravikumar, Department of Electronics & Communication, Dayanand Sagar College of Engineering, VTU, Banglore, India.

Dr. K. L. Sudha, Department of Electronics & Communication, Dayanand Sagar College of Engineering, VTU, Banglore, India.

DSSS can also be used as a multiple access technique like CDMA, wherein several different pseudorandom spreading codes are being used for different users.

II. GENERATION OF PN SEQUENCES

1. Legendre sequence: These sequences are to be any prime length and are based on quadratic residues (qr). The Legendre symbol is a multiplicative function with values 1, -1, 0 that is a quadratic character modulo prime number p.

a is qr of p $\Longleftrightarrow$ x^2 mod p = a has a solution a

The Legendre symbol is a function of 'a' and 'p' defined as follows:

$$(a/p) = \begin{cases} 1 \text{ if a is quadratic residue modulo P and } a \equiv 0 (\text{mod } p) \\ -1 \text{ if a is quadratic non-residue modulo P} \\ 0 \text{ if } a \equiv 0 \text{ (mod P)} \end{cases}$$

ON-THE-FLY CODE GENERATION: Let $\mathbf{L_n = [L_{n-1} + (2n-1)] \text{ mod } p}$, where L_n=Sequence indices: L_1 =1 & n->2 to (p-1) and p is prime length. L_n is sequence indices at which ones occur. The Legendre sequence (LS) may then be defined [2] as

$$LS(k) = \begin{cases} 1 & \text{if } k \in \{L_n\} \\ -1 & \text{if } k \notin \{L_n\} \end{cases} \qquad k \rightarrow 0 \text{ to } (P-1)$$

2. Weil sequence: A Weil code (a; w) is specified by the Weil index w, ranging from 1 to (p-1)/2, where p is length of Legendre sequence and is a prime [6]. Each Weil sequence is obtained by performing EX-OR of Legendre sequence and a circular shift of Legendre sequence.

$$W_i(a; w) = LS(a) \oplus (LS((a+w) \text{ mod } p))$$

3. Sidel'nikov sequence: Let 'p' be an odd prime and 'm' be a positive integer. Let $\mathbf{F_p^m}$ be the finite field with p^m elements and 'α' be a primitive element of $\mathbf{F_p^m}$. The Sidel'nikov sequence [11]

$\mathbf{S = \{s(t); t=0, 1, 2\ldots\ldots\ldots\ldots P^m - 2\}}$ of period $P^m - 1$ is defined by

$$s(t) = \begin{cases} 1 & \text{if } (\alpha^t + 1) \in N \\ 0 & \text{otherwise} \end{cases}$$

where N→ set of quadratic non-residues over finite field $\mathbf{F_p^m}$ and are represented as

$$N = \{\alpha^{2t+1}; t = 0, 1, 2\ldots\ldots\ldots ((p^m-1)/2)-1\}$$

m→ positive integer

α→ primitive element

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

4. M-ary Sidel'nikov sequence: Let $\mathbf{F_q}$ be a finite field with $\mathbf{q = p^m}$ and 'M' a divisor of q-1, where 'p' is a prime and 'm' is a positive integer. Let 'α' be a primitive element in F_q and $\mathbf{D_k = \{\alpha^{Mi+k}\text{-}1 | 0 \leq i < (q\text{-}1)/M\}}$ **for** $\mathbf{0 \leq k \leq (M\text{-}1)}$

Then M- ary Sidel'nikov sequence: $\mathbf{S = \{s(t) | 0 \leq t \leq (q\text{-}2)\}}$ of period q-1 is defined by **[7]**

$$S(t) = \begin{cases} 0 & \text{if } \alpha^t = -1 \\ k & \text{if } \alpha^t \in D_k \end{cases}$$

III. PERFORMANCE ANALYSIS OF PN SEQUENCES

These involves seven tests [12] to check the randomness of the PN sequences as follows

1. The Frequency (Monobit) test:

Function call: n → The length of the bit string, Ɛ → $Ɛ_1$, $Ɛ_2$……. $Ɛ_n$

Test Description:

i. Conversion to ±1: The zeros and ones of the input sequence (Ɛ) are converted to values of -1 and +1 and are added together to produce $S_n = X_1+X_2+\ldots\ldots\ldots\ldots X_n$, where $X_i = 2Ɛ_i\text{-}1$.

ii. Compute the test statistic $S_{obs} = |Sn| / \sqrt{n}$.

iii. Compute p-value = erfc ($S_{obs} / \sqrt{2}$).

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random.

2. Frequency Test within a Block:

Function call: Block Frequency (M, n) where; M → The length of each block, n → The length of the bit string, Ɛ → $Ɛ_1$, $Ɛ_2$……. $Ɛ_n$

Test Description:

i. Partition the input sequence into N = [n/M] non-overlapping blocks. Discard any unused bits.

ii. Determine the proportion π_i of ones in each M-bit block using the equation

$$\pi i = \sum_{j=1}^{M} \frac{Ɛ_{(j-1)M+j}}{M} \qquad \text{for } 1 \leq i \leq N$$

iii. Compute the χ^2 static: $\chi 2(obs) = \sum_{i=1}^{N} (\pi i - 1/2)^2$

iv. Compute the p-value = igamc (N/2,χ^2 *(obs)/2).*

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random.

3. The Runs Test: Function call: Runs (n), where; n → The length of the bit string, Ɛ → $Ɛ_1$, $Ɛ_2$……. $Ɛ_n$

Test Description:

i. Compute the pre-test portion π of ones in the input sequence: $\pi = \Sigma_j Ɛ_j/n$

ii. Determine if the prerequisite frequency test is passed: If it can be shown that $|\pi\text{-}(1/2)| \geq \tau$, then the Runs test need not be performed (i.e. the test should not have been run because of a failure to pass test 1, the Frequency test). If the test is not applicable, then the p-value is set to 0.0000. Note that for this, $\tau = 2/\sqrt{n}$ has been pre-defined in the test code.

iii. Compute the test statistic:

$$v_n(obs) = \sum_{k=1}^{n-1} r(k) + 1$$ where r (k) =o if $Ɛ_k = Ɛ_{k+1}$, and r (k) =1 otherwise.

iv. Compute p-value= $erfc\left(\frac{|v_n(obs) - 2n\pi(1-\pi)|}{2\sqrt{2n\pi(1-\pi)}}\right)$

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random.

4. Tests for the Longest-Run-of-Ones in a Block:

Function call: Longest Run of ones (n), where; n → The length of the bit string, Ɛ → $Ɛ_1$, $Ɛ_2$……. Ɛ, M→ The length of each block. The test code has been pre-set to accommodate three values for M: M=8, M=128, $M=10^4$ in accordance with the values of sequence length n (minimum) i.e. 128, 6272,750,000 respectively, N→ The number of blocks

Test Description:

i. Divide the sequence into M-bit blocks.

ii. Tabulate the frequencies v_i of the longest runs of ones in each block into categories.

iii. Compute test statistic:

$$\chi^2(obs) = \sum_{i=0}^{k} (vi - N\pi i)^2 / N\pi i$$

iv. Compute p-value = igmac (k/2 , χ^2/2)

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random

5. The Binary Matrix Rank Test:

Function call: Longest Run of ones (n), where; n → The length of the bit string, Ɛ → $Ɛ_1$, $Ɛ_2$……. $Ɛ_n$, M→ The number of rows in each Matrix, Q→ The number of columns in each matrix

Test Description:

i. Sequentially divide the sequence into M.Q-bit disjoint blocks; there will exist N= [n/MQ] such blocks.

ii. Determine the binary rank (R_l) of each matrix, where l=1…N.

iii. Let F_M=the number of matrices with R_l=M (full rank), F_{M-1}=the number of matrices with R_l=M-1(full rank-1), $N\text{-}F_M\text{-}F_{M-1}$=the number of matrices remaining.

iv. Compute

$$\chi^2(obs) = ((F_M\text{-}0.2888N)^2/(0.2888N)) + ((F_M\text{-}0.5736N)^2/(0.5736N)) + ((N\text{-}F_M\text{-}F_{M-1}\text{-}0.133N)^2/(0.2888N))$$

v. Compute p-value = igamc (1, χ^2(obs)/2)

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random.

6. The Non-overlapping Template Matching Test:

Function call: Non-overlapping template matching (m,n), m→The length in bits of each template,n →length of entire bit string under test, Ɛ→ $Ɛ_1$..... $Ɛ_n$, B →m-bit template to be matched, M →length in bits of the substring of Ɛ to be tested, N →the number of independent blocks.

Test description:

i. Partition the sequence into N independent blocks of length M

ii. Compute the theoretical mean and variance:

$\mu = (M\text{-}m+1)/2^m$ $\sigma^2 = M(1/2^m - 2m\text{-}1/2^{2m})$

iii. Compute test statistic:

$$\chi^2(obs) = \sum_{j=1}^{N} (Wj - \mu)^2 / \sigma^2$$

iv. Compute p-value = igamc (N/2, χ^2(obs)/2)

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random

7. The Overlapping Template Matching Test:

Function call: Non-overlapping template matching (m,n), m →The length in bits of each template,n →length of entire bit string under test, Ɛ → $Ɛ_1$..... $Ɛ_n$,

B →m-bit template to be matched, M → length in bits of the substring of Ɛ to be tested, N →the number of independent blocks.

Test Description:

i. Partition the sequence into 'N' independent blocks of length M.

ii. Calculate the number of occurrences of B in each of the N blocks (v_i)

iii. Calculate λ and η values: $\lambda=(M-m+1)/2^m$, $\eta=\lambda/2$

iv. Compute test statistic :

$$\chi^2\ (obs) = \sum_{i=0}^{5}(vi - N\pi i)^2 / N\pi i$$

vi. Compute p-value= igamc (5/2, χ^2(obs)/2)

Note: If p-value <0.01, then conclude that the sequence is non-random. Otherwise, conclude that sequence is random.

IV. SIMULATION RESULTS

The simulation of all PN sequences and their Randomness tests are performed in MATLAB 2009b and results as follows

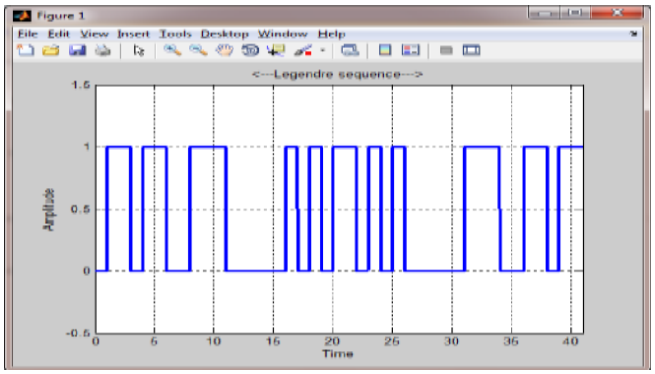

Fig. 1 Legendre Sequence (Prime Length=41)

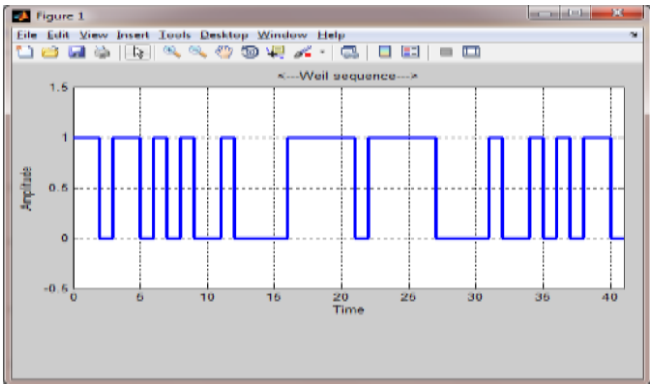

Fig. 2 Weil Sequence (Prime Length=41)

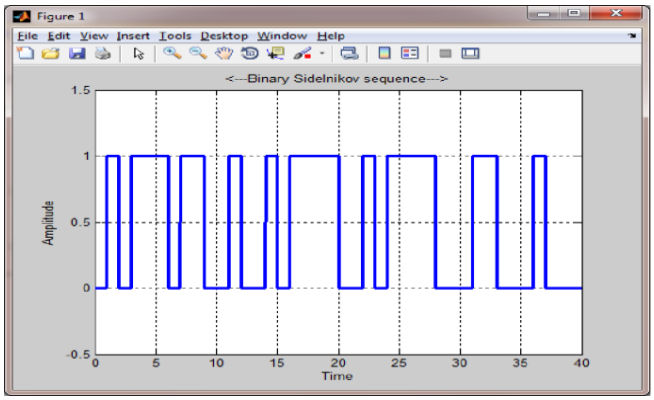

Fig. 3 Sidel'nikov Sequence (Prime Length=41, m=1)

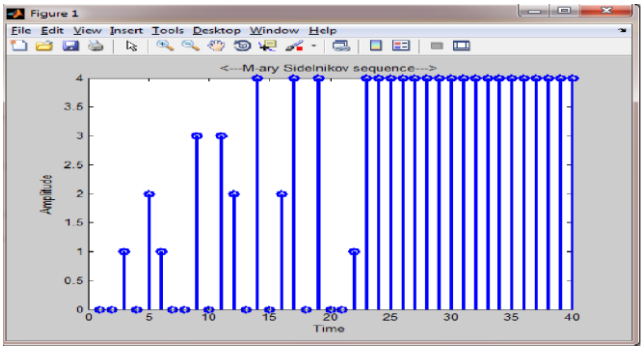

Fig. 4 M-ary Sidel'nikov Sequence (Prime Length=41, m=1, M=5)

TESTS	Legendre Sequence	Weil Sequence	Sidel'nikov Sequence
Test 1	0.97539	0.97539	1
Test 2	0.40090	0.53141	0.72353
Test 3	0.92624	0.92624	1
Test 4	0.55796	0.25510	0.45819
Test 5	0.29191	0.29191	0.29191
Test 6	0.55361	0.66941	0.85836
Test 7	0.93882	0.95199	0.94546

Table I Randomness Tests (Prime Length=1051)

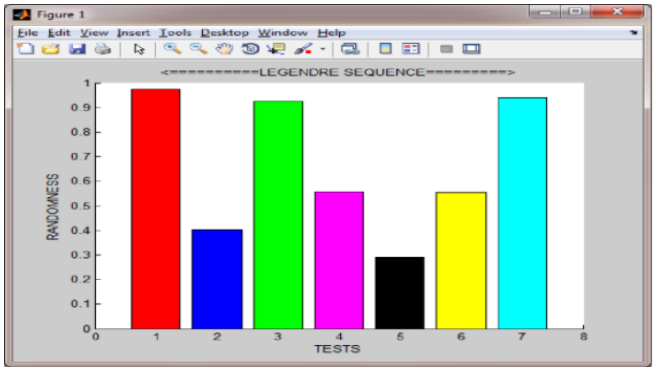

Fig. 5 Legendre Sequence (Randomness Tests)

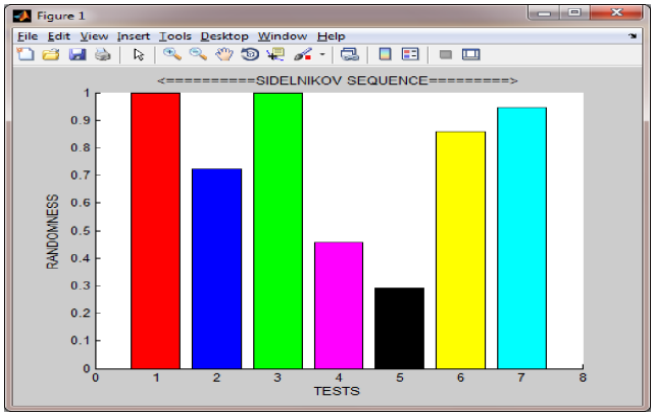

Fig. 6 Weil Sequence (Randomness Tests)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

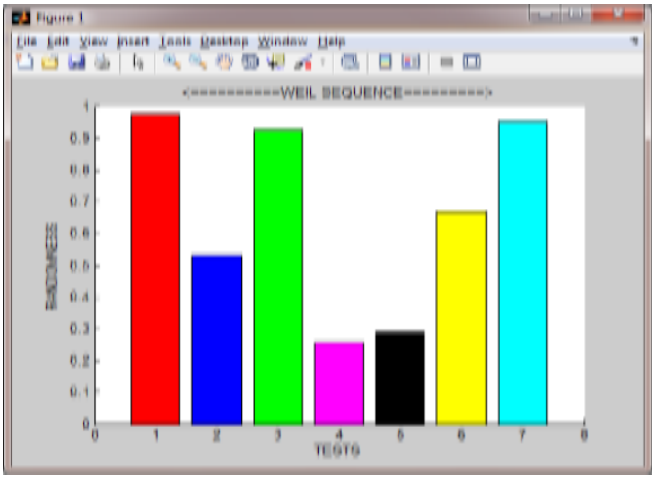

Fig. 7 Sidel'nikov Sequence (Prime Length=41)

V. CONCLUSION

The PN sequences i.e. Legendre sequence, Weil sequence, Sidel'nikov sequence and M-ary Sidel'nikov sequence are generated, and the first three binary sequences are used for Spread spectrum communication. And performing all Randomness Tests for binary PN sequences, it can be concluded that the sequences are Random i.e all randomness values of all tests obtained for all binary PN sequences are more than the value 0.01, then can be concluded that, binary PN sequences are random in nature.

ACKNOWLEDGMENT

The satisfaction that accompanies any task is incomplete without naming the people who made it possible and whose constant guidance and encouragement made to work perfect. I consider it a great privilege to extend my heartfelt gratitude to **Dr. K L SUDHA,** Department of Electronics and Communication Engineering, Dayananda Sagar College of Engineering, Bangalore, for her kind co-operation, constant motivation, encouragement and assistance throughout this paper.

REFERENCES

1. Hui Lu and Ruiyao Niu (school of electronic & information Engineering, Beihang university). Generation method of GPS L1C codes based on quadratic reciprocity law.
2. P. Mumford, E. Glennan and N. Shivaramaiah (university of New South Wales, Australia). An Investigation of correlator Design Architecture to support QZSS L1 signals.
3. Young-Sik Kim, Ji-woong Jang, Jong-Seon No, sang- Hyo Kim. New Quaternary sequences with Ideal Auto correlation constructed from Legendre sequences.
4. R.G.Van schyndel, A.Z. Tirkel, I.D.svalbe (Depatment of physics, Manash University, Clayton, 3168, Australia). Key Independent Watermark Detection.
5. Stefan Wallner, Jose-Angel Avila-Rodriuez, Guenter W.Hein (university FAF Munich, Germany). Galileo E1 OS and GPS L1C pseudo Random Noise codes.
6. Joseph J. Rushanan (the MITRE Corporation, Bedford, 01730, USA). Weil sequences: A Family of Binary sequences with Good correlation properties.
7. Nam Yul Yu and Guang Gong (Department of Electrical & computing engineering, university of waterloo). Multiplicative characters, the Weil Bound, and polyphase sequences families with low correlation.
8. Young-Sik Kim, Jung-Soo Chung, Jong-Sean No. On the Autocorrelation Distributions of Sidel'nikov sequences, IEEE Transactions of Information Theory, VOL. 51,No.9,September 2005.
9. Dae san Kim, Member: IEEE. A family of sequences with large size and good correlation property arising from M-ary Sidel'nikov sequences of period q^d-1, Journal of latex Class Fields, Vol.6,No.1, January 2007.
10. Nam Yul Yu and Guang Gong (Lakehead University). New construction of M-ary sequence Families with low correlation from the structure of Sidel'nikov sequences.
11. Yu-Chang Eun, Hong-Yeop Song and Gohar M. Kyureghyan, One-error linear complexity over F_p of Sidel'nikov sequence.
12. NIST (National institute of standards and Technology), a statistical Test suite for Random and pseudorandom Number Generators for cryptographic Applications, April 2010, Lawrence E bass ham 111
13. Alfred J.Menezes, Paul C. Van Oorschot, scoot A.Vanstone, HANDBOOK of APPLIED CRYPTOGRAPHY.

AUTHORS PROFILE

Cheruku Ravikumar, received B.E Degree in Electronics and Communication from Visvesvaraya Technological University in 2011, Currently Pursuing M.Tech Degree in Digital Electronics and Communication from Visvesvaraya Technological University in 2014, Department of Electronics and Communication, Dayanand Sagar College of Engineering, Bangalore, India. Main Interests in Digital Communications.

Dr. K L Sudha, Department of Electronics and Communication, Dayanand Sagar College of Engineering, Bangalore, India.