# Design and Implementation of Weil Sequence and LDPC Codes.

Rajagopal A[1] ,Vedha S[2]

[1]*(Assistant Professor, Dept. of Electronics and Communication, Dayananda Sagar College of Engineering, Bangalore, India, gopiluck@gmail.com)*

[2]*(PG Scholar, Dept. of Electronics and Communication, Dayananda Sagar College of Engineering, Bangalore, India, svedha92@gmail.com)*

**ABSTRACT:** CDMA is a digital wireless technology that makes use of spread spectrum technique to access the communication channel.This paper presents Weil pseudo random noise sequence and LDPC error control coding technique. A base band signal communication system is been designed using Weil pseudo random noise sequence as spreading sequence and LDPC error control coding technique as channel encoder and decoder. The entire system is realised using System generator.

**KEYWORDS:** CDMA, GNSS, LDPC error control coding, LDPC simplified soft distance decoding, PRN sequence, Weil sequence.

## I. INTRODUCTION

Global navigation satellite system (GNSS) is a system of satellites that provide geo-spatial positioning of an object with global coverage.In 1970s the U.S.Department of Defence developed the first navigation system which became fully operational in 1995. In addition to GPS the other satellite positioning systems that are now operating or planned are: GLONASS (Russia), Galileo (European Union), Compass (China), IRNSS (India) and QZSS (Japan) [1]. The GNSS satellites transmit the navigation signals in two or more frequencies in L-band.The IRNSS uses CDMA technique to access the channel.

CDMA technique allows several users to share a band of frequencies to transfer the information. In order to avoid interference amongst the multiple users the CDMA employs spread spectrum technique where the original information is spread to a much larger bandwidth using pseudo random noise (PRN) sequence.CDMA technique is employed in GPS application where PRN sequences are used in order to differentiate the messages transmitted by respective satellites. Further, for reliable transmission of these data over channel, error control coding techniques are employed at the transmitter and receiver end. Rapid advances in electronic deviceshave enabled the implementation of very powerful error control coding techniques whose performance is very close to Shannon's limit [3].

The new modernised GPS civilian signals are L2C signal, L5 signal and L1C signal. The satellites designed to operate in L1C band use Weil PRN sequence as spread sequence and LDPC error control coding [10]. However which LDPC technique is employed is not being described. This paper presents a simple baseband communication system design which uses Weil Sequence and LDPC simplified soft distance decoding technique.

The organisation of the paper is: Section II consists of the background work related to design the system, Section III describes the design of Weil sequence, Section IV describes the design of LDPC encoder and simplified soft distance decoder, Section V shows the block diagram, Section VI shows the implementation results and Section VII describes the future work and concludes the paper.

## II. BACKGROUND WORK

The pseudo random noise sequence are used in CDMA systems to spread the data bits to much higher bandwidth at the transmitter end and de-spread the received bits at the receiver end to get back the original data bits. The present method employed in generation of PRN sequence is by using linear feedback shift register (LFSR).This method of generation of PRN sequences have good correlation property but do not provide flexibility in their length as it depends on the number of shift registers.The present PN sequences used which is based on LFSR are Maximal length codes, Gold codes [4], Bent function and Kasami codes. Prime length based sequences such as Legendre sequence and Weil sequences have a good correlation properties and are said to exist for any prime length giving more flexibility [2] [6].

The present error control coding techniques used are: hamming code, cyclic redundancy check (CRC), Bose–Chaudhuri–Hocquenghem (BCH) for satellite communication and other applications, Reed–Solomon (RS) codes in storage devices, satellite communication systems and other applications[3]. Low Density Parity Check (LDPC) codes are finding interesting use in applications where reliability is prime factor. LDPC codes are said to closely approach the Shannon's limit [3] [5] [7].

Decoding in LDPC is an iterative process.The decoding are of two types: Hard decision decoding and soft decision decoding. In hard decision decoding, the decision making is based on threshold value whereas in soft decision decoding the decision making is based on probability. Soft decision decoding of LDPC uses Sum-product algorithm to decode the erroneous bits. However this algorithm involves sum and product of floating point variables. As the number of iterationincreases the hardware complexity increases. Soft distance metrics such as the Euclidean distance gives maximum likelihood of transmitted information thus giving the best estimation of transmitted bits [8]. Soft distance decoding involves sum and differences of floating point variables and thus reduces the hardware complexity.

## III. WEIL PN SEQUENCE

Weil codes are based on the Legendre sequence. Legendre sequence are constructed using quadratic residues [2].Quadratic residues can be found using Euler's criterion [9].

According to *Euler's criterion*, for any integer 'b' such that gcd (b, p) =1 where 'p' is a odd prime, if

$$b^{(p-1)/2} \equiv 1 \ (\text{mod } p) \qquad (1)$$

then 'b' is quadratic residue of 'p'

andif

$$b^{(p-1)/2} \equiv -1 \ (\text{mod } p). \qquad (2)$$

then 'b' is quadratic non-residue of odd prime 'p'.

Example: Let us consider a prime number 13.The quadratic residues for prime number 13 are

$1^{(6)} \equiv 1$ (mod 13)

$2^{(6)} \equiv -1$ (mod 13)

Performing the similar operation for all the values till 13, we get,

The quadratic residues for prime number 13 as R={1,3,4,9,10,12} and non-residues NR={2,5,6,7,8,11}.

The Legendre symbol for 'p' odd prime number and integer 'b' is defined as [2]

$$\left(\frac{b}{p}\right) = \begin{cases} 0, & b=0 \\ 1, & b \text{ is a quadratic residue mod p} \\ -1, & b \text{ is a quadratic non residue mod p} \end{cases} \qquad (3)$$

Thus the Legendre symbol for p=13 is L={-1, 1,-1, 1, 1,-1,-1,-1,-1, 1, 1,-1, 1}

where b=0 is always 0 and is represented as 1.

Weil sequence is generated by performing xor operation on Legendre sequence and shifted version of itself [2]. The generation of Weil sequence is shown in [9], and thus the Weil sequence for prime number 'p=13' is W={1,1,1,1,0,1,0,0,0,1,0,1,1}.

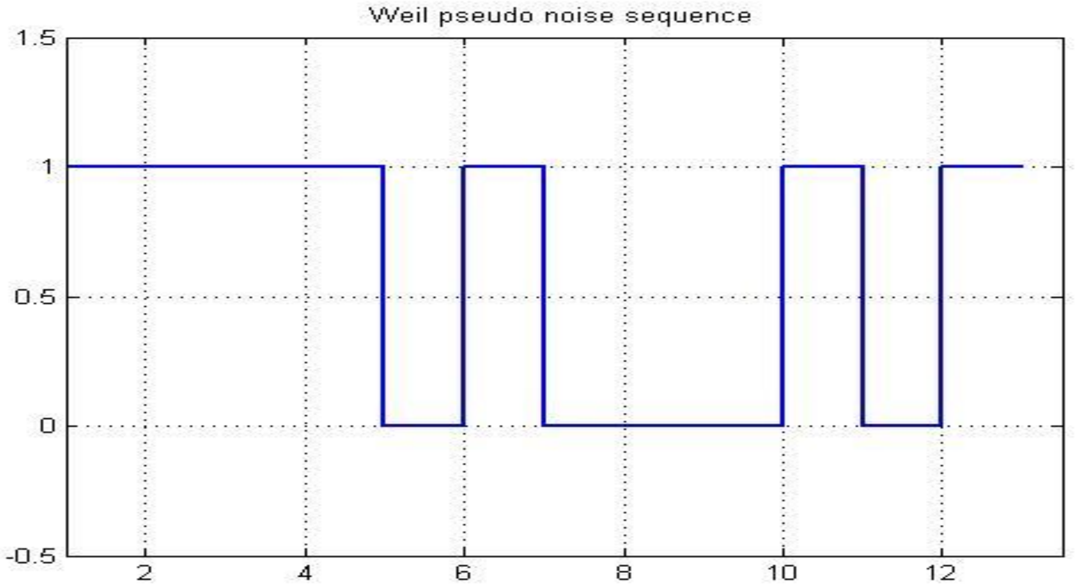


Figure 1: Weil sequence generation for prime number 13 in Matlab.

## IV. LDPC CODES

The LDPC codes are the one which has parity check matrix with few number of 1's when compared to 0's.

LDPC encoder encodes the 'k' message bits with Generator matrix of size k x n to get an 'n' bit codeword.

$[C]_{1 \times n} = [m]_{1 \times k} * [G]_{k \times n}$ (4)

where C is the codeword, m is the message bits and G is the generator matrix.

The LDPC decoder uses H matrix to decode the bits received at the receiver end. The LDPC simplified soft distance decoder uses Euclidean distance as its metrics to decode the erroneous bits [8].The detail explanation of the algorithm for LDPC simplified soft distance is described in the reference paper [8].

The summary of simplified soft distance decoding is as follows:

Step1:The soft (Euclidean) distance of the received bits with 0 and 1 is calculated at the variable node end.

Step 2: The horizontal step involves the computation of minus of log of sum of the antilog of their negative distances at the check nodes. The resulting values are combined with the Tanner graph.

Step 3: The vertical step updates the values at the variable node with the values received from check nodes that is computed in step 2.

Step 4: The decision step compare the values and decides if the received bit is 0 or 1.

It is shown that the simplified soft distance decoding doesn't need the information of SNR at the decoder input and the performance is almost equivalent to LogSP algorithm [8].

The bit error rate ratio versus signal- to - noise ratio is calculated for H matrix of size (8 x 12), (64 x 96) and (504 x 1008), this is shown in Fig. 2, Fig.3 and Fig.4.

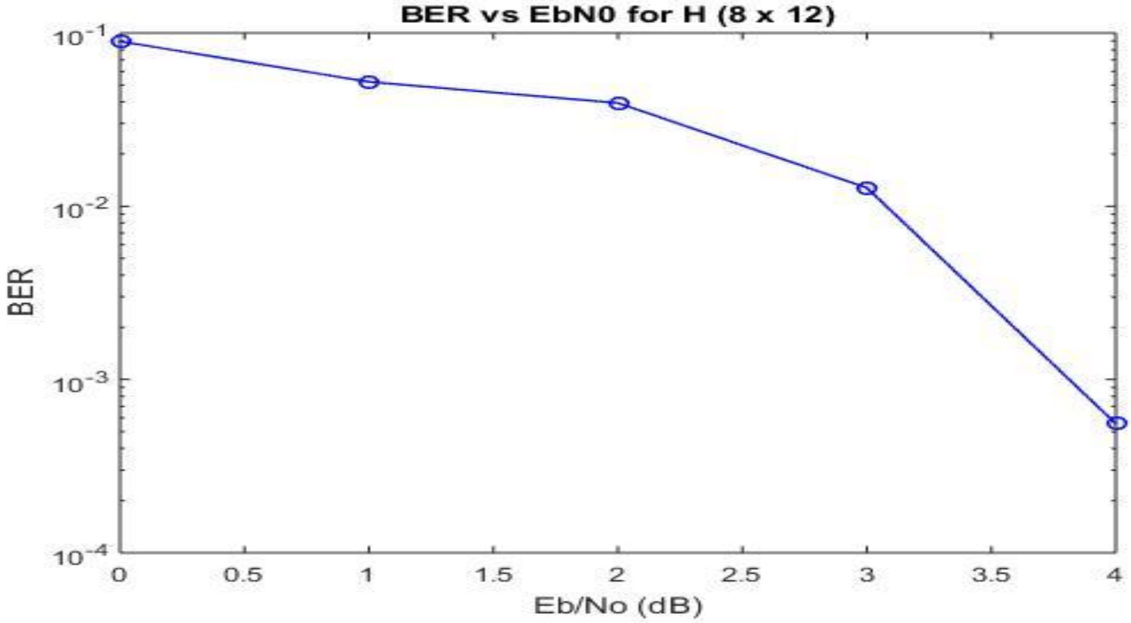


Figure 2: BER vs. EbN0 plot for H matrix of size 8 x 12.

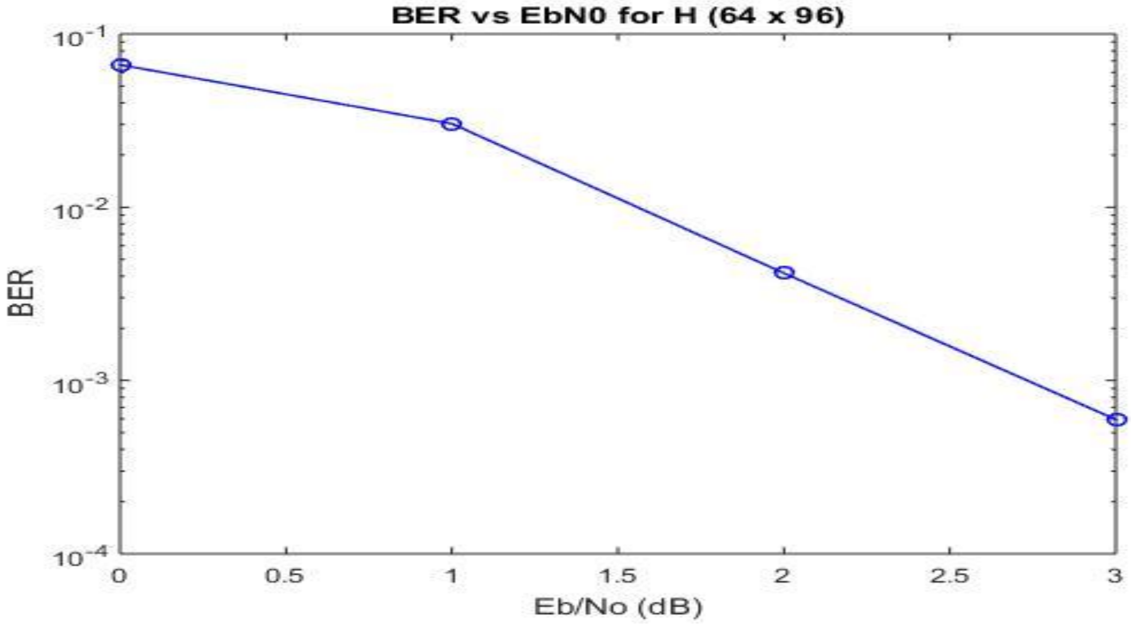


Figure 3: BER vs. EbN0 plot for H matrix of size 64 x 96.

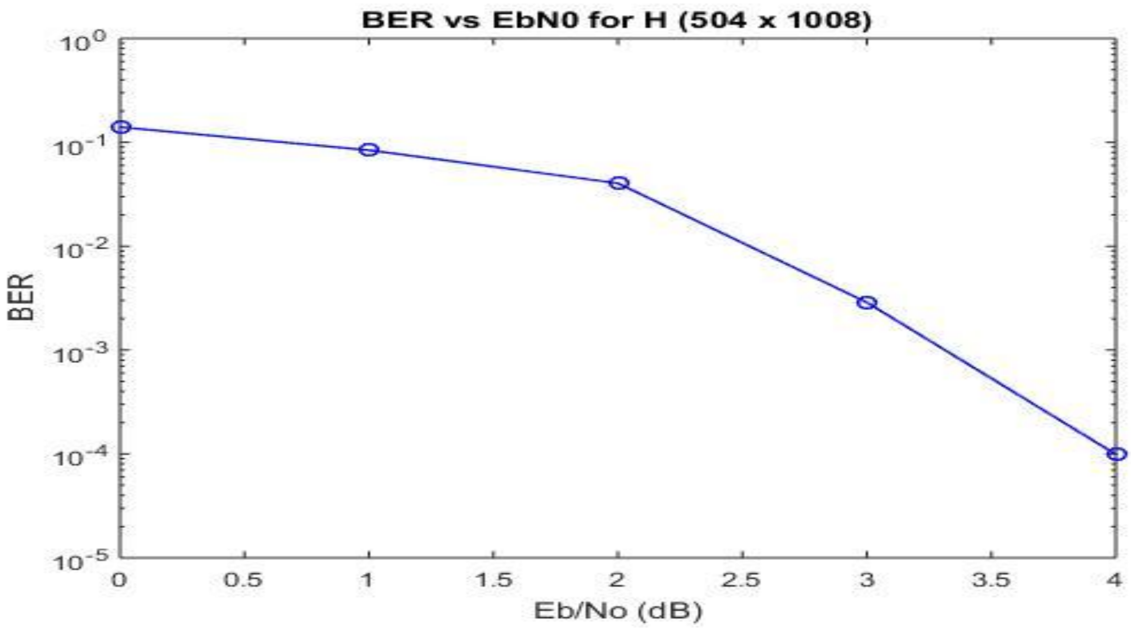


Figure 4: BER vs. EbN0 plot for H matrix of size 504 x 1008.

## V. BLOCK DIAGRAM

This section describes the communication system design forbaseband signal transmission. Weil PN sequence is usedto spread the message bits to higher bandwidth. The spread sequence is given to a LDPC encoder which encodes the bits with Generator matrix. The encoded bits are transmitted over a noisy channel. The LDPC soft decision decoder decodes the erroneous bits using H matrix and retrieves the bits. The decoded bits are further multiplied with Weil sequence to reproduce the message.

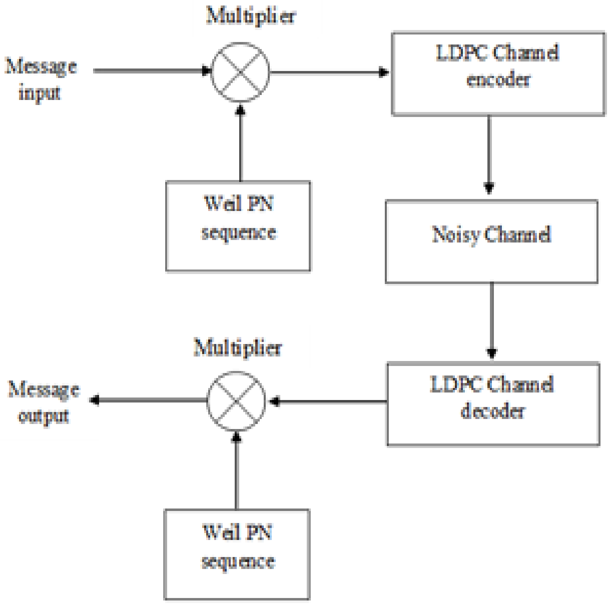


Figure 5: Communication system design for transmission of baseband signal.

The Fig. 6 below shows how the data sequence is spread to a higher bandwidth sequence. The data sequence is multiplied with the pseudo random noise sequence at the transmitter side to give a spread sequence that has a higher bandwidth than the original message sequence.

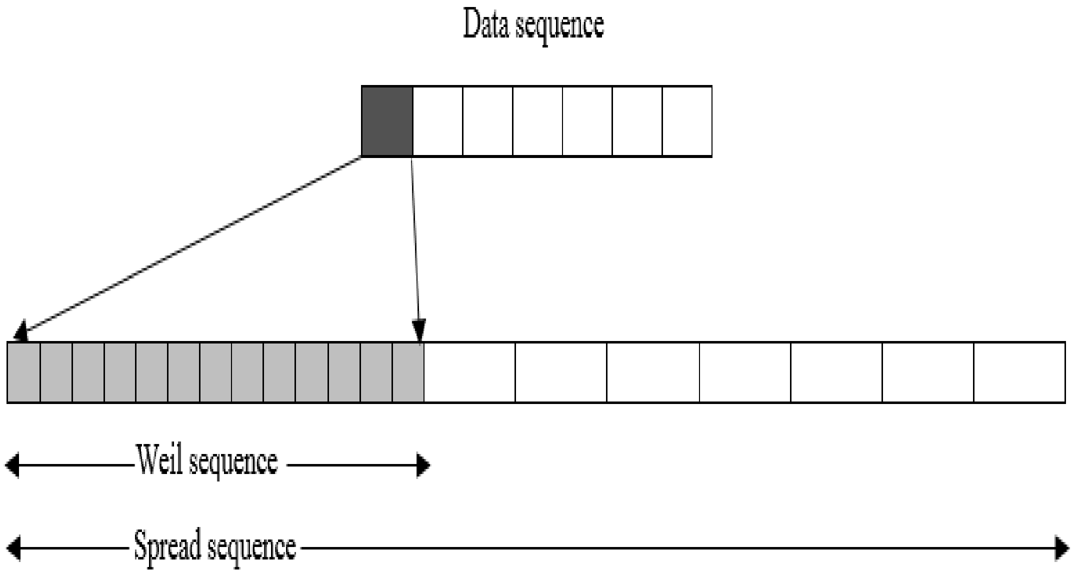
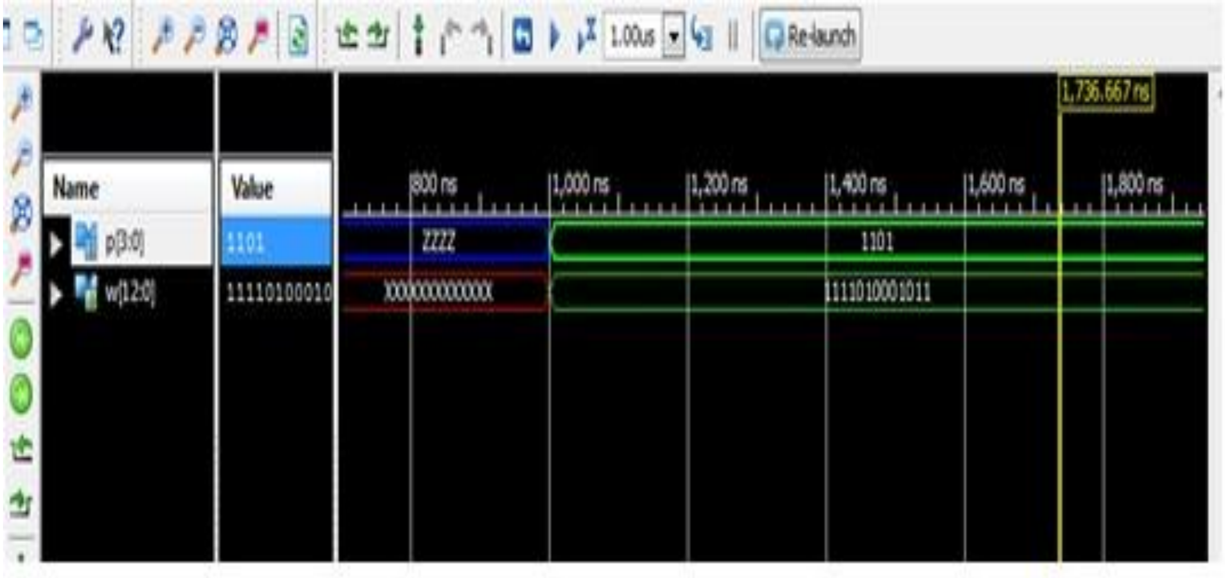


Figure 6: Spread spectrum sequence.

After the sequence is spread, the encoder block encodes the spread sequence with the generator matrix. The G matrix used are of dimensions (4 x 12), (32 x 96) and (504 x 1008). The encoded bits are passed through a noisy channel to receiver. The decoded decodes the erroneous bits using LDPC matrix. The dimensions of H matrix used are (8 x 12), (64 x 96) and (504 x 1008).
Further the decoded sequence is de-spread to retrieve the original data sequence sent.

## VI. IMPLEMENTATION RESULTS

The Weil sequence is generated for prime number 13. The simulation results obtained in Xilinx 14.2 is shown in Fig.7.



| Name | Value |
|---|---|
| p[3:0] | 1101 |
| w[12:0] | 11110100010 |

Figure 7: Weil sequence generation in Xilinx ISE 14.2 Simulator.

The entire system for baseband signal communication with Weil pseudo noise sequence and LDPC error control coding is realized in Matlab. The Verilog code for Weil sequence is written and the LDPC code in Matlab.The entire design is implemented on Atlys Spartan 6 FPGA board using System Generator.

The different combinations of data sequence, Weil sequence, G matrix, H matrix, signal-to-noise ratio (Eb/N0) that is used and implemented on FPGA is shown in Table I. below.

| *Data sequence* | *Weil sequence* | *G matrix dimension* | *H matrix dimension* | *EbN0 in dB* |
|---|---|---|---|---|
| 32 bits | 31 bits | 4 x 12 | 8 x 12 | 2 |
| 7 bits | 13 bits | 32 x 96 | 64 x 96 | 0.9 |
| 32 bits | 31 bits | 504 x 1008 | 504 x 1008 | 2 |

Table I: Different combinations of data sequence, Weil sequence, G matrix, H matrix, signal-to-noise ratio (EbN0) that is used in the design.

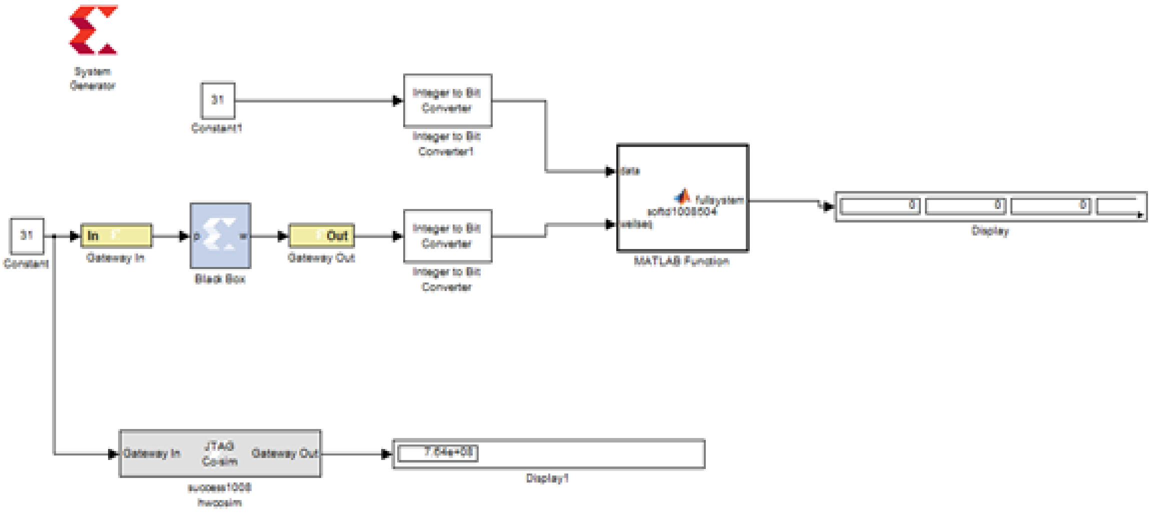


Figure 8: System design implementationon Spartan 6 using System Generator.

## VII. CONCLUSION

This paper shows the design of Weil sequence and LDPC simplified soft distance decoding algorithm. Weil sequence and LDPC error control coding is presently been used in GPS L1C satellites. The Weil sequence is designed using Verilog HDL and implemented on Artix 7 FPGA board. The entire system is implemented on Atlys Spartan 6 FPGA board using System Generator.The future work includes realising the entire system on FPGA kit, comparing the performance of different LDPC soft decision decoding algorithms such as sum-product algorithm, LogSP algorithm, and soft distance algorithm and extending the system for a prime number based PRN sequence of 10230 bits which is presently used in L1C satellites.

## REFERENCES

[1]. Shuanggen Jin, *Global Navigation Satellite Systems- Signal, Theory and Applications* (Published by InTech, Janeza, Trdine 9, 51000 Rijeka, Croatia, 2012).

[2]. J. J. Rushanan, "Weil Sequences: A Family of Binary Sequences with Good Correlation Properties," in IEEE International Symposium on Information Theory, Seattle, WA, pp. 1648 – 1652, 2006.

[3]. Jorge Castiñeira Moreira, Patrick Guy Farrell,*essentials of error-control coding* (John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England).

[4]. Yong-Hwan Lee and Seung-Jun Kim, “Sequence Acquisition of DS-CDMA Systems Employing Gold Sequences”,IEEE Transactions On Vehicular Technology, Vol. 49, No. 6, November 2000 2397.

[5]. Robert G Galleger,*Low density parity check codes*, Cambrige, Mass., July 1963.

[6]. Jong-Seon No, Hwan-Keun Lee, Habong Chung, Hong-Yeop Song, Kyeongcheol Yang, Trace, “Representation of Legendre Sequences of Mersenne Prime Period”, IEEE Transactions on Information Theory, Vol. 42, No. 6, November 1996.

[7]. D.J.C. Mackay and R.M. Neal, “Near Shannon limit performance of low density parity check codes,” Electronics Letters, vol. 33, pp 457-458 (1997).

[8]. P.G. Farrell1, L.J. Arnone2 J. Castin˜ eira Moreira3, “Euclidean distance soft-input soft-output decoding algorithm for low-density parity-check codes”,IET Commun., 2011, Vol. 5, Iss. 16, pp. 2364–2370

[9]. A. Rajagopal, K.L. Sudha, Dundi Ajay,” FPGA Implementation of Pseudo Noise Sequences based on Quadratic Residue Theory”, International Journal of Computer Applications (0975 – 8887) Volume 134 – No.9, January 2016.

[10]. “Global Positioning Systems Directorate Systems Engineering & Integration, Interface Specification, IS-GPS-800”, September 24, 2013.