International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

Design and Analyze the various m-sequences codes in MATLAB

Anshul Khatter[1], Poonam Goyal[2]
[1,2] *Asst. prof., Apeejay Stya University, Sohna- Palwal Road, Sohna, Gurgaon*

Abstract **— Pseudo noise sequences (PN) are widely used in telecommunications and for measurement purposes. In this paper, cross correlation results of PN family codes: Gold, Kasami sequences are shown. PN sequences have random like properties that help in reducing the correlation among speech samples. In Spread Spectrum CDMA system each user is assigned a pseudo noise sequence for the purpose of spreading as well as despreading. The maximal length PN-sequence (m-sequence) is the best-described PN-sequence whose length is equal to its period. Various PN-codes can be generated using Linear Feedback Shift Register (LFSR). All the results presented here were tested and simulated via MatLab programs. In modern communication systems, spread spectrum is playing an increasingly important role day by day due to its inherent advantages like noise immunity and also due its practical applications like mobile communications in CDMA. A comparison of PN sequence, Gold sequence, Kasami sequence is studied. The SNR Performance of Gold, Kasami & M-sequence of sufficiently long periods are close to that of the purely random and independent binary sequence of same length.**

Keywords **— Autocorrelation, Gold Sequence, Kasami Sequence, MATLAB, m-sequence, PN sequence, Spread spectrum communication.**

I. INTRODUCTION

When transmitting information through insecure channels, some method is used convert the intelligible data into unintelligible form prior to transmission and this process of conversion with a key is called encryption. At the receiver side, the encrypted message is converted back to the original form by the process called decryption [1]. In DS-CDMA method, users are multiplexed by distinct codes and all users use the same bandwidth. For de spreading operation, the receive data should multiplied with the same code in the receiver. So the other user codes in the same frequency band must be uncorrelated with the desired user code. This is the reason DS-CDMA codes have to be designed so as to posses very low cross-correlation.

With the advancement of VLSI technology spread spectrum CDMA system has now come up as a highly emerging digital technology for mobile systems [11]. Spread Spectrum modulation techniques are defined as those techniques in which the bandwidth of the transmitted signal is much greater than the bandwidth of the original message, and the bandwidth of the transmitted signal is determined by the message to be transmitted and by an additional signal known as the Spreading Code [13].

As there are complex channel conditions like attenuation and interference, the PN-Code will often be received with some PN-Code chips corrupted. A chip is a fraction of a packet or even a bit. [2]. PN sequences are used as the frame head to develop enhanced channel estimation (CE) algorithm for Multiple Input Single Output co-channel interference cancellation [3].

In this paper, m-sequences, Pseudo Noise sequences, Gold sequences and Kasami sequences are discussed. Pseudorandom sequences have been commonly used in various fields like communications, navigation, radar technology, cipher technologies, remote control, measurements, and industrial automation [4]. The maximal period sequences (m-sequences) and their decimations are used to design sequence families with low-correlation [5]. PN sequences are streams of 1's and 0's [6].

PN Sequence Generator generates a sequence of pseudorandom binary numbers by using shift register, as shown in Figure1. The m-sequence generator is generally constructed with linear feedback shift registers (LFSR) [7]. The PN sequence generator is generally made up of shift registers with feedback [9]. By linearly combining elements from taps of the shift register and feeding them back to the input of the generator, a sequence of much longer repeat length using the same number of delay elements in the shift register are obtained, therefore these blocks are also referred to as LFSR 10].Gold Sequences are generally generated by the modulo-2 operation of two different m-sequences of same length [8].

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

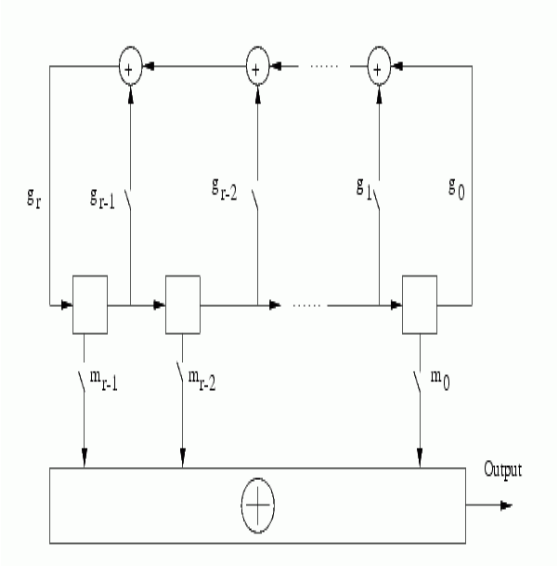

Figure1. M-Sequence Generator Structure [16]

Autocorrelation and cross correlation of PN codes are important functions to evaluate the performance of spread spectrum communication systems [12]. The increasing importance of application areas like cryptography and spread-spectrum communications has led to an interest in periodic correlation parameters for pseudorandom sequences. For this kind of systems, there is a generation of a noise-like signal. Most cryptographic areas need the implementation of pseudo-random periodic sequences with high cross-correlation properties [14]. Gold sequences defer the minimum cross-correlation values that can possibly expect from periodic m-sequences. Other type of sequence defined is Kasami sequences which are set of sequences having good cross correlation properties. Two classes of Kasami sequences are there: small and large sets. The small set of Kasami sequences are optimal sequences, these sequences have better correlation properties compared to Gold sequences [8]. The large set contains all the sets sequences in the small sets [15]. The large set contains more number of sequences compared to Gold codes but these sequences have more correlation values compared to Gold codes [8].

The remainder of this paper is organized as follows: Section II presents the material and method of the designed system for generation of m sequence, Gold sequence, Kasami sequence and its autocorrelation in MATLAB. Section III gives a detailed discussion on the results obtained.

The final section concludes and describes the future scope of this work.

II. Material And Method

To generate PN sequence, Gold sequence, Kasami sequence MATLAB v 7.5 is used. A PN sequence is generated by means of a linear feedback shift register and is determined by the length m of the shift register, its initial state and the feedback logic.

Firstly, NRZ encoder is used to get encoding data streams. Polar method of encoding is used in this paper, two other methods of encoding are Manchester & unipolar. This data stream is used to generate m-sequence & then autocorrelation of generated m-sequence is simulated & measured theoretically. Then find autocorrelation of m-sequence by simulation. Autocorrelation also be calculated theoretically.

Period of an m-sequence is defined by

$$N=2^m-1$$

m- Length of the shift register.

Let c (t) is the resulting waveform of the maximum-length sequence. Period of the waveform c (t) is

$$T_b=N\,T_c$$

T_c is the duration assigned to symbol 1 or 0 in the maximal-length sequence.

Autocorrelation function of a periodic signal c (t) of period T_b is

$$R_c(\tau) = \frac{1}{T_b}\int_{-T_b/2}^{T_b/2} c(t)c(t-\tau)\,dt$$

Where the lag τ lies in the interval (-Tb /2, Tb /2).Using this formula autocorrelation is represented as

$$R_c(\tau) = \begin{cases} 1 - \dfrac{N+1}{NT_c}|\tau|, & |\tau| \le T_c \\ -\dfrac{1}{N}, & \text{for the remainder of the period} \end{cases}$$

[16,17]

Gold sequences of length N are constructed from a preferred-pair of m-sequences and the mod 2 sums of these preferred pair of m-sequences.

Kasami sequences are obtained by decimating the m-sequence and performing mod-2 addition on cyclically shifted sequences.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

Gold and Kasami have certain pairs of m-sequences of length n where it exhibit a three-valued cross-correlation function with values {-1; - t(m); t(m) -2}, where

$$t(m) = 2^{(m+1)/2} + 1 \text{ (odd m)}$$

$$2^{(m+2)/2} + 1 \text{ (even m)}$$

Resultant sequences are called preferred sequences [18]. Preferred sequences are utilised to produces many well known families of binary sequences with good cross-correlation properties like Gold and Kasami sequences.

In the same way, smaller set of Kasami sequence having $M = 2^{m/2}$ binary sequences of period $n = 2m - 1$, where m is even, is generated [19]. The maximum cross-correlation value for any pair of sequences from the set is

$$2^{m/2} + 1 \qquad [19]$$

III. Results And Discussions

The resultant PN sequence & polar format of generated PN sequence is shown in Figure2. This figure shows that number of binary 0s are differ by number of 1s by one chip only, which is the property of m-sequence. In figure, first part shows generated m-sequence with respect to chip index and second part shows when this generated m-sequence is coded in polar format. In polar format, output is shown with respect to time.

Figures 3 & 4 show the comparison of autocorrelation function of m-sequence simulated values with measured values of autocorrelation function for different values of lag. These autocorrelation plots shows the number of agreements minus disagreements for the overall length of the two sequence (one is generated m-sequence and other is its time shifted sequence).

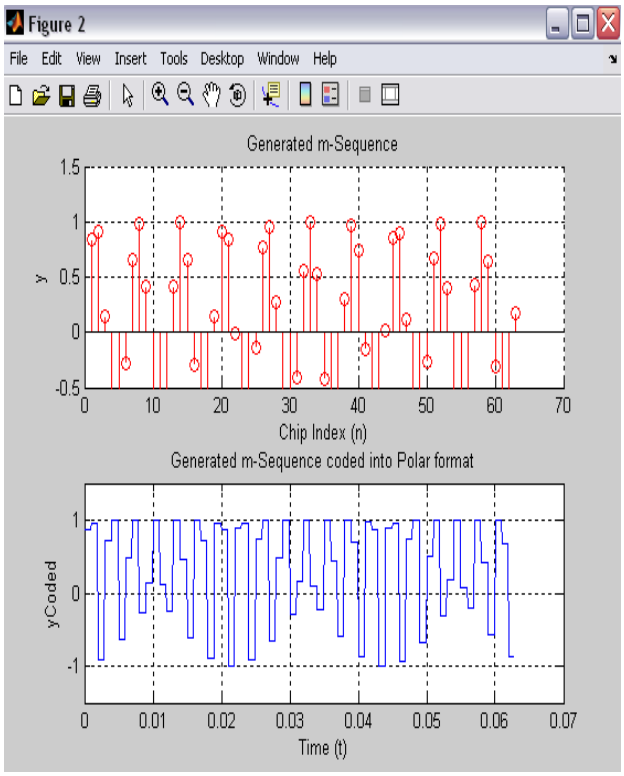

Figure2. Generated m-sequence & its polar format

Figure 3 shows autocorrelation function when the polynomial is x^3+x^1+1.This figure shows that for autocorrelation functions increases or decreases linearly with the lag so autocorrelation function is triangular.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

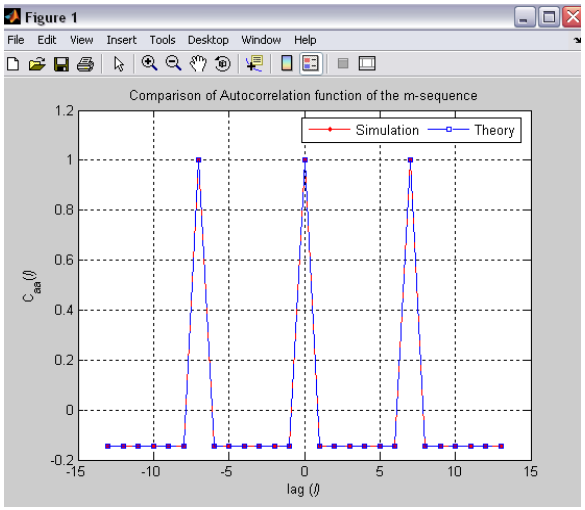

Figure3. Comparison of theoretical & simulation values Of autocorrelation for N=3

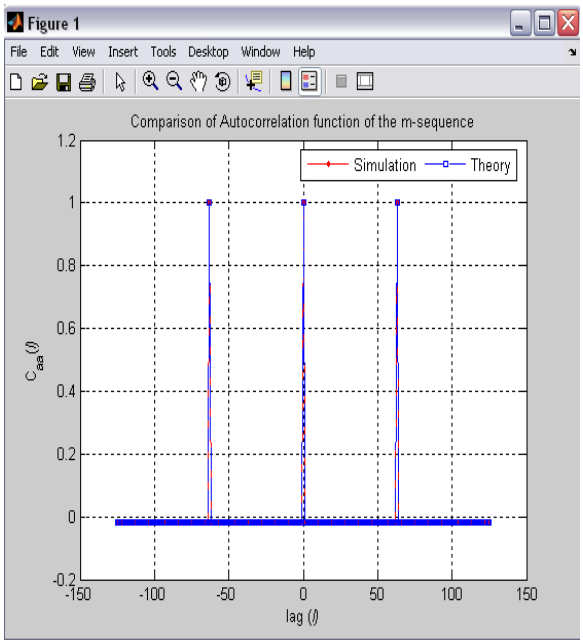

Figure4. Comparison of theoretical & simulation values Of autocorrelation for N=6

Figure 4 shows autocorrelation function when the polynomial is x6+x1+1. This figure shows that when the degree of polynomial increases autocorrelation function gives spike values.

The increase in the degree of polynomial demands for more number of shift registers cascaded linearly as shown in fig 1.The above result shows that as the polynomial degree are increased the Tc (chip rate of sequence) increases rapidly thereby increasing the frequency spectrum which in turn generates spikes.

Figure5 shows cross correlation and autocorrelation of two different generated gold sequences (codes).In the first part of figure, cross correlation of two different generated gold codes are shown. In the second part Autocorrelation of Sequence1 (0 0 0 0 0 0 1 1, 1 0 0 1 0 0 0 1) is shown & in the third part Autocorrelation of sequence2 (0 0 1 0 1 0 1 1, 0 1 1 1 0 0 1 1)is shown.In each sequence number of codes is 2 having code length 8.

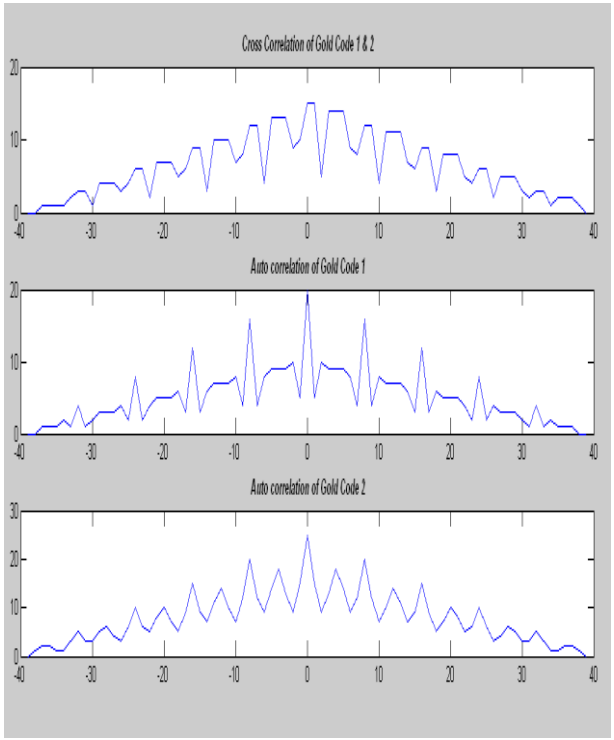

Figure5. Cross correlation & Auto correlation two Gold Codes

This figure shows that Gold codes from different Gold code groups have bad correlation properties, even when synchronized.

Figure6 shows the cross correlation for small set of Kasami.

International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 11, November 2012)

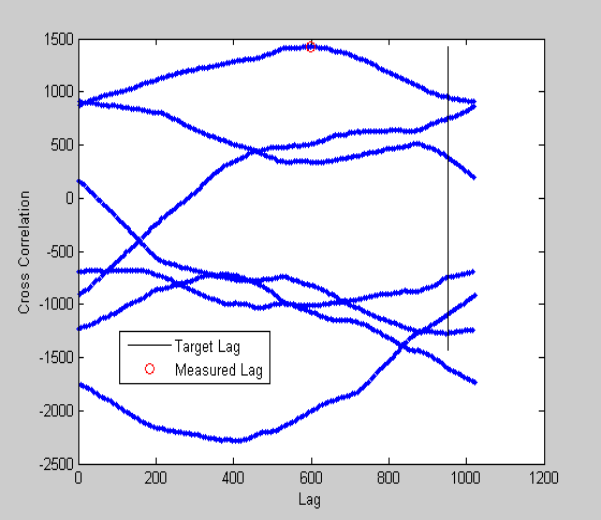

Figure6. Cross correlation of small set of Kasami sequences

This figure shows the target lag & the measured lag of small set of Kasami sequence.

IV. Conclusion And Future Work

The system proposes an effective use of PN m-sequence, Gold sequence & Kasami sequence in the one of the most versatile techniques of Spread Spectrum popularly known as DSSS. The above scheme shows that the autocorrelation coefficients of PN m-sequence are well suited for Spread Spectrum as application in DSSS used in W-CDMA. However, a comparison of simulated & measured value proves that it has excellent autocorrelation property. It also shows longer Gold sequences will perform better as SSMA sequences & Kasami sequences have low cross correlation property than Gold sequences & that's why Kasami sequences are used in scrambling code in W-CDMA systems.

REFERENCES

[1] W. Diffe and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. 22, pp. 644-654, Nov. 1976.

[2] Kaishun Wu, Haoyu Tan,Hoi-Lun Ngan, IEEE, Yunhuai Liu, and Lionel M. Ni, "Chip Error Pattern Analysis in IEEE 802.15.4", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 4, APRIL 2012.

[3] Jian Xiong, Lin Gui, Huafen Liu, and Peng Cheng, "On Channel Estimation and Equalization in 2X 1 MISO TDS-OFDM Based Terrestrial DTV Systems", IEEE TRANSACTIONS ON BROADCASTING, VOL. 58, NO. 1, MARCH 2012.

[4] Soo Yun Hwang, Gi Yoon Park, Dae Ho Kim, and Kyoung Son Jhang, "Efficient Implementation of a Pseudorandom Sequence Generator for High-Speed Data Communications" , ETRI Journal, Volume 32, Number 2, April 2010.

[5] Lei Hu, Xiangyong Zeng, Nian Li, Wenfeng Jiang, "Period-Different m-Sequences With at most a four-valued cross correlation" http://arxiv.org/abs/0801.0857

[6] V. Anil Kumar, Abhijit Mitra and S. R. Mahadeva Prasanna, "On the Effectivity of Different Pseudo-Noise and Orthogonal Sequences for Speech Encryption from Correlation Properties" , World Academy of Science, Engineering and Technology 48 2008

[7] A. Fuster and L. J. Garcia, "An efficient algorithm to generate binary sequences for cryptographic purposes," Theoretical Computer Science, vol. 259, pp. 679-688, May 2001.

[8] Abhijit Mitra," On Pseudo-Random and Orthogonal Binary Spreading Sequences", World Academy of Science, Engineering and Technology 48 2008

[9] Soo Yun Hwang, Gi Yoon Park, Hyeong Jun Park, and Kyoung Son Jhang, "AN IMPROVED IMPLEMENTATION METHOD OF THE GOLD SEQUENCE GENERATOR".

[10] "Gold Code Generator Reference Design," Altera Application Note 295, March 2003.

[11] F.Simpson and J. Holtzman, "CDMA power control, interleaving, and coding", Proc. 41st IEEE Vehic. Technol. Conf., Saint Louis, MO, pp. 362-367,1991

[12] A. K. Elhakeem, G. S. Takhar, and S. C. Gupta, "New code acquisition techniques in spread spectrum communications", IEEE Trans. Commun., vol. COM-28, pp. 246-259, Feb. 1980

[13] Abid Yahya, Othman Sidek, and Junita Mohamad-Saleh, "Design and Develop Wireless System Using Frequency Hopping Spread Spectrum", Engineering Letters, 13:3, EL_13_3_6

[14] F. Rodríguez Henríquez, N. Cruz Cortés , J.M. Rocha-Pérez , "GENERATION OF GOLD-SEQUENCES WITH APPLICATIONS TO SPREAD SPECTRUM SYSTEMS"

[15] S.Kalita, P.P Sahu, " A New Modified Sequence Generator for Direct Sequence Spread Spectrum (DSSS)", National Conference on Electronics, Communication and Signal Processing, NCECS-2011,19th September 2011

[16] Wireless Network Evolution 2G to 3G by Vijay K.Garg,Pearson Education

[17] Anshul Khatter, Parikshit Vasisht ,Nithya Suseelan, "A Purposed Scheme to Exhibit Spread Spectrum in DSSS Using m-sequences PN code in MATLAB" , National Conference on Future Mobile Radio Systems,17thSeptember 2011,FET, MRIU, Faridabad

[18] R. Gold, \Maximal Recursive Sequences with 3-valued Recursive Cross Correlation Functions," IEEE Trans. Inform. Theory, vol. IT-14, pp. 154-156, January 1968.

[19] T. Kasami, \Weight Distribution Formula for Some Class of Cyclic Codes," Tech.Report No. R-285, Univ. of Illinois, 1966.