GOLD PSEUDORANDOM SEQUENCE GENERATION USING LINEAR FEEDBACK SHIFT REGISTER FOR INTERLEAVER IN 5G MOBILE COMMUNICATION SYSTEM

Dr. Tran Canh Duong
Hoa Binh University
Corresponding Author: tcduong@daihochoabinh.edu.vn

Ngày nhận: 02/5/2024
Ngày nhận bản sửa: 10/5/2024
Ngày duyệt đăng: 19/6/2024

Abstract

Interleaved Division Multiple Access (IDMA) can support a large number of users within the same bandwidth and can achieve high data rates but does not require too much complexity in designing the transceiver process using VLSI. In this paper, the author use an effective mathematical tool to describe Pseudorandom Noise-PN which is finite field theory and D transform, then develop an algorithm to generate pseudo-random sequences to implement to generate code for an interleaver for use in a 5G mobile communication system.

Keywords: *LFSR-Linear Feedback Shift Register, Gold pseudorandom sequence, interleaver, deinterleaver, IDMA-Interleaved Division Multiple Access.*

Tạo chuỗi giả ngẫu nhiên Gold sử dụng thanh ghi dịch chuyển phản hồi tuyến tính cho bộ xen kẽ trong hệ thống truyền thông di động 5G

TS. Trần Cảnh Dương
Trường Đại học Hòa Bình
Tác giả liên hệ: tcduong@daihochoabinh.edu.vn

Tóm tắt

Đa truy cập phân chia xen kẽ (IDMA) có thể hỗ trợ một số lượng lớn người dùng trong cùng một băng thông và hỗ trợ đạt được tốc độ dữ liệu cao nhưng không đòi hỏi quá phức tạp trong việc thiết kế quy trình thu phát bằng VLSI. Trong bài viết này, tác giả sử dụng một công cụ toán học hiệu quả để mô tả nhiễu giả ngẫu nhiên-PN, đó là lý thuyết trường hữu hạn và biến đổi D, sau đó, phát triển thuật toán tạo chuỗi giả ngẫu nhiên để triển khai tạo mã cho bộ xen kẽ sử dụng trong hệ thống thông tin di động 5G.

Từ khóa: *Thanh ghi dịch chuyển phản hồi tuyến tính (LFSR), chuỗi giả ngẫu nhiên Gold, bộ xen, bộ giải xen, đa truy cập phân chia xen kẽ (IDMA).*

1. Introduction

Interleave Division Multiple Access (IDMA) is one of the Non-orthogonal multiple access (NOMA) techniques. IDMA is a special form of Code Division Multiple Access (CDMA). In the IDMA system, the receiver distinguishes each station by their unique interleaving patterns instead of unique spreading codes. This leads to a low complexity receiver [3]. As the number of parallel stations increases, the complexity increases linearly, so this research result has a certain meaning [3]. A single carrier for Multi-layer IDMA system for long-term development of 3GPP (LTE) system has been proposed [4]. This system has advanced features throughput and reliability from CDMA systems. In addition, IDMA has several other advantages over orthogonal frequency division multiple access (OFDMA) and CDMA. Thus, IDMA has higher spectral efficiency and is not sensitive to clipping deformation A. IDMA OVER CDMA [1]. Different modulation ways like Binary Phase Shift Keying (BPSK), Quadrature Phase Shift Keying (QPSK) can be applied to IDMA [8]. This article covers data rate enhancement for IDMA.

A. NOMA techniques and IDMA over CDMA

Non-orthogonal multiple access (NOMA) has features such as enhanced spectrum efficiency, reduced latency, high speed, reliability, and massive connectivity. NOMA can serve multiple users with the same resources in time, frequency, and space. NOMA can be widely applied in the fifth generation (5G), includes Machine-to-Machine communication and Internet of Things (IoT). Issues related to coding, modulation and channel estimation also needs to be revised. IDMA is one the technique relies on different interleavers for separations signals from different users in the spectrum span multiple users of the communication system. CDMA is an all-use spread spectrum technique spectrum, which users in the channel are uniquely identified by Pseudo-random numbers help increase voice and data capacity. Thus, CDMA can accommodate more users at any given time instantly. Serious limitations of CDMA is interference multiple access. DMA is uniquely assignable interleaving set for each user. This is different from allocation of different frequency bands, different time slots and the spread spectrum chains in FDMA, TDMA and CDMA respective systems. The IDMA system is considered a special system case of CDMA system where the interleaving index is assumed code string to identify the user.

B. IDMA transmitter and IDMA receiver

Figure 1. shows the transmitter structure of an IDMA system with multiple user [2].

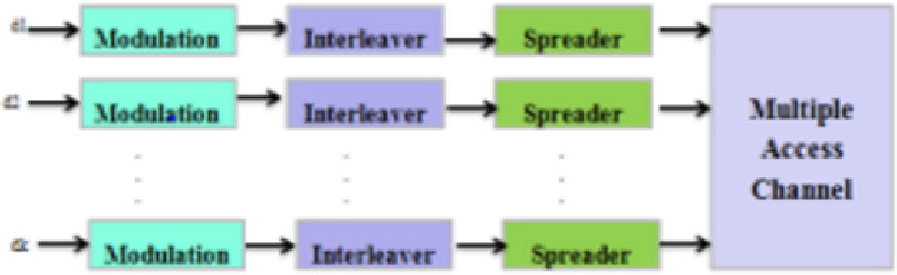


Figure 1. The transmitter structure of an IDMA system with multiple user

The input data sequence of user is modulated using Binary Phase Shift Key technique (BPSK). BPSK is a two phase modulation scheme, where the 0's and 1's in a binary message are represented by two different symbols in the carrier signal. The input bit binary 0 is represented by +1 and input bit binary 1 is represented by -1. Next, the aggregated modulation bits are permuted using a random interleaver. Users are distinguished only by their random code, which is determined from the interleaver. Figure 2 depicts the data shuffling random interleaver different users with different patterns. An interleaver is a device which rearranges the ordering of a data sequence by means of a deterministic bijective mapping [7]. An interleaver maps C onto a sequence $X = [x_0, x_1, \ldots x_{N-1}]$ where X is the permutation of the elements of C.

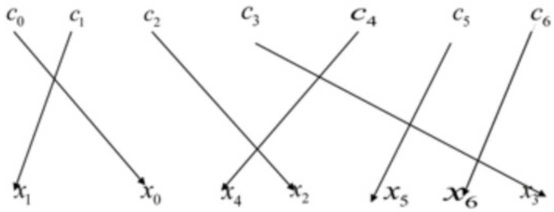


Figure 2. Mechanism of data interleaving

C and X are an N-dimensional pair vector. There is a correspondence $c_i \mapsto x_j$ between each element of C and each element element of X. The mapping function can be expressed as an ordered set called interleaving vector p.

p = [p(0), p(1),…p(N-1)]. $X^k = B^{p(k)}$ is the kth element of the permuted sequence X.

Interleaver and deinterleaver

At the receiver, the inverse interleaver, i.e. the deinterleaver, is responsible for restoring the permuted sequence to to its original order. Thus the separation of users defined by user-specific interleavers. The user-specific interleavers are generated independently and randomly. In a mobile communication system, the base station must use one significant amount of memory to store random codes. For proper decoding of the sequence of interleaver, the receiver must have all the relevant information regarding pattern of interleaving at transmitter side. Therefore, in order to operate IDMA scheme properly, base station has to forward the information of interleaving at the receiver side of the system.The IDMA receiver consists of multiuser detection, despreader, deinterleaver, and demodulator. Each block in the receiver is used to retrieve back the original data sent by every user. The Figure 3 shows the IDMA receiver structure [2].

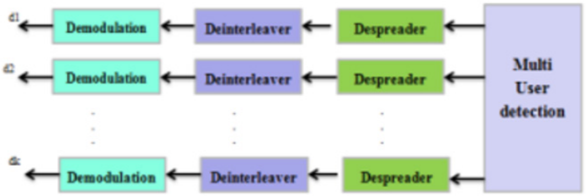


Figure 3. IDMA Receiver block diagram

2. Generate a pseudo-random signal for interleaver

An effective mathematical tool for describing Pseudorandom Noise-PN sequences is finite field theory and the D transform. The elements of the Galois field (GF(p)) are represented by integers 0,1,2,...,p-1 [5]. We can use the d transform to describe the signal sequences and also the hardware of the Linear Feedback Shift Register, because the D transform is a transform that can be easily deduced from the mathematical expression to binary and vice versa. Alternating m sequences can be generated by the transform D [10]. The D transformation of a string b_n over GF(p) is represented by D[bn]:

$$D[b_n] = \sum_{i=0}^{n} b_i d^i , b_i \epsilon \{GF(p)\}$$

The D transform of the series will have polynomial form in terms of d on GF(p) and has been conveniently used in signal and system analysis in data transmission [6][11]. The transform D of the generator sequence b_n of the linear feedback shift register (LFSR) is then given by the equation:

$$b(d) = \frac{s(d)}{g(d)}$$

where g(d) of degree n is the generation polynomial of LFSR and S(d) of degree no more than n – 1 specifies an initial condition corresponding to a particular shifted version of b_n. When g(d) is a primitive polynomial, the sequence {bn} is generated with the largest period length. In this case, b_n is called the maximal length sequence or m sequence [9][10]. The sequence m has period 2^m-1, where m is the degree of the generating polynomial. The sequence m satisfies the equilibrium property and the run length property, making them appear random.

Figure 4. shows Gold chain generator diagram example, which combines two m sequences the m corresponding to polynomials $x^6+x^5+x^2+x+1$ and $x^6+x^5+x^3+x^2+1$.

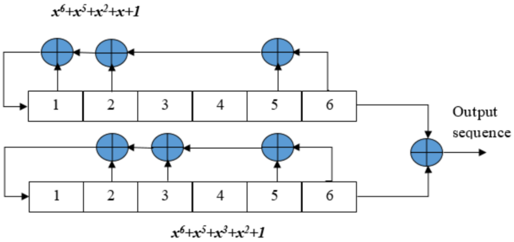
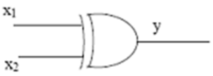


Figure 4. Gold chain generator diagram

Figure 5. depicts the notation, formula, and truth table of the modular adder.

$$y = x_1 \oplus x_2 = \bar{x}_1 x_2 + x_1 \bar{x}_2$$



x_1	x_2	y
0	0	0
0	1	1
1	0	1
1	1	0

Figure 5. The notation, formula, and truth table of the modular adder [2].

The algorithm for generating sequences done in the following steps [9]:

1) Choose a primitive polynomial.

2) Generate the PN sequence corresponding to the selected primitive polynomial. Store all S −1 shifts of this sequence. Generate a PN sequence of length S =2 ^{m} −1 for some integer m using a linear feedback shift register with the connections defined by a primitive polynomial of degree m over the Galois field GF(2).

3) Add the ordered bitwise modulus of the pseudo-random sequence m corresponding to the generating polynomials to increase the number of nonlinearly nested PN codes in the case that all PN sequences have the same degree m.

We use the following program:

clear all; close all;

x1=[1 1 1 1 1 1]; n1 = length(x1); len1 = 2^n1-1; p1(1,1) = x1(1,1);

z1 = x1; for y1 = 2 : len1x1 = z1; for i = 1 : n1 if (i==1) z1(1,i) = xor (x1(1,1), xor (x1(1,2), xor (x1(1,5), x1(1,6)))); else z1(1,i) = x1(1,i-1); end p1(1,y1) = z1(1,6); end subplot 211;

stem (p1);

Figure 6 shows the pseudorandom sequence m with the generating polynomial is $x^6+x^5+x^2+x+1$.

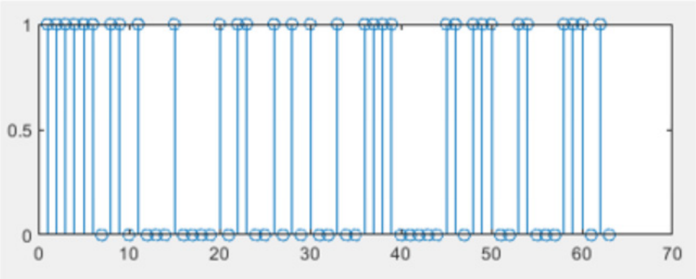


Figure 6. The pseudorandom sequence m with the generating polynomial is $x^6+x^5+x^2+x+1$.

The bit sequence X_1 is as follows:

We use the following program:

1 1 1 1 1 1 0 1 1 0 1 0 0 0 1 0 0 0 0 1 0 1 1
0 0 1 0 1 0 1 0 0 1 0 0 1 1 1 1 0 0 0 0 0 1
1 0 1 1 1 0 0 1 1 0 0 0 1 1 1 0 1 0 0.

clear all; close all; x1=[1 1 1 1 1 1]; n1 = length(x1); len1 = 2^n1-1; p1(1,1) = x1(1,1);

z1 = x1; for y1 = 2 : len1 x1 = z1; for i = 1 : n1 if (i==1)

z1(1,i) = xor (x1(1,2), xor (x1(1,3), xor (x1(1,5), x1(1,6)))); else z1(1,i) = x1(1,i-1); end

end p1(1,y1) = z1(1,6); end subplot 211; stem (p1);

Figure 7 shows the pseudorandom sequence m with the generating polynomial is $x^6+x^5+x^3+x^2+1$.

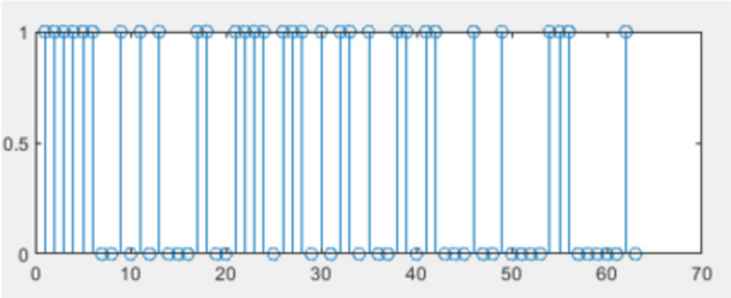


Figure 7. The pseudorandom sequence m with the generating polynomial is $x^6+x^5+x^3+x^2+1$.

The bit sequence X_2 is as follows:

1 1 1 1 1 1 0 0 1 0 1 0 1 0 0 0 1 1 0 0 1 1 1
1 0 1 1 1 0 1 0 1 1 0 1 0 0 1 1 0 1 1 0 0 0
1 0 0 1 0 0 0 0 1 1 1 0 0 0 0 0 1 0 0.

Modularly adding two pseudo-random sequences m, we have the output sequence of the Gold code as follows:

$$Z = X_1 \oplus X_2$$

Z = 0000000100001000110110010010000100111000110010010100101101110000.

Follow the logic circuit example in Figure 4, preferred pair m-sequences generated by preferred pair polynomials $x^6+x^5+x^2+x+1$ and $x^6+x^5+x^3+x^2+1$ of the same order n = 6 have the following period:

$$L = 2^6\text{-}1=64\text{-}1=63$$

Two m sequences create 65 (=63+2) Gold chains with the same period L. The first two sequences in the set are m-sequences, but the rest are not and they do not have the properties of m-sequences.

When the actual 5G mobile communication network needs to increase the number of random pseudocodes, we can use a Linear Feedback Shift Register with a higher order generation polynomial. For example, Simulate with a polynomial of degree m=10.

$$x^{10}+x^6+x^5+x^3+x^2+x+1$$

The simulation program is as follows:

```
clear all; close all; x1=[1 1 1 1 1 1 1 1 1 1]; n1 = length(x1); len1 = 2^n1-1;
p1(1,1) = x1(1,1); z1 = x1; for y1 = 2 : len1 x1 = z1; for i = 1 : n1 if (i==1)
z1(1,i)=xor(x1(1,1),xor(x1(1,2),xor(x1(1,3),xor(x1(1,5),xor(x1(1,6),x1(1,10))))));
else z1(1,i) = x1(1,i-1); end end p1(1,y1) = z1(1,10); end subplot 211; stem (p1);
```

Figure 8 depicts the result of an m-sequence generated by a linear feedback shift register with a generating polynomial of $x^{10}+x^6+x^5+x^3+x^2+x+1$.

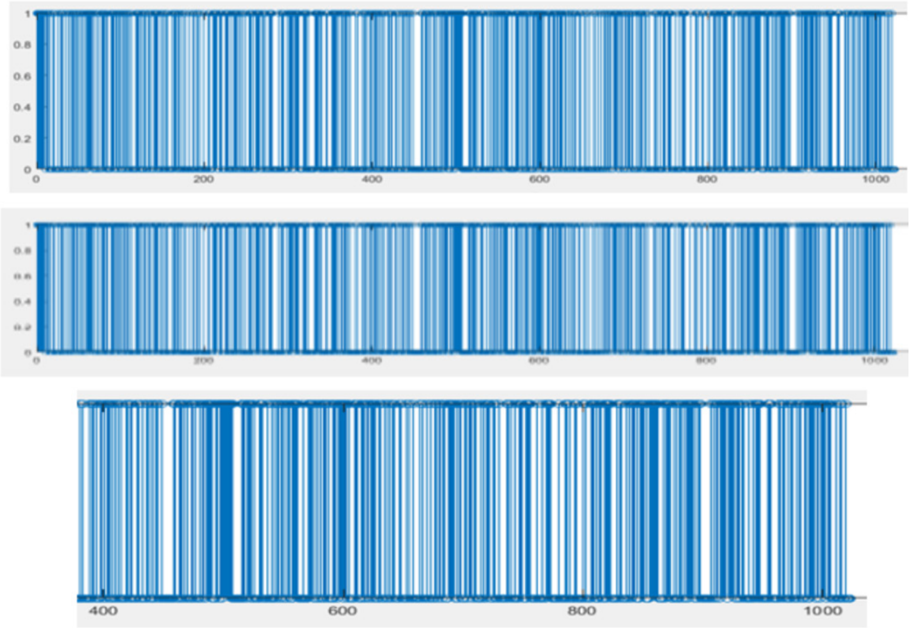
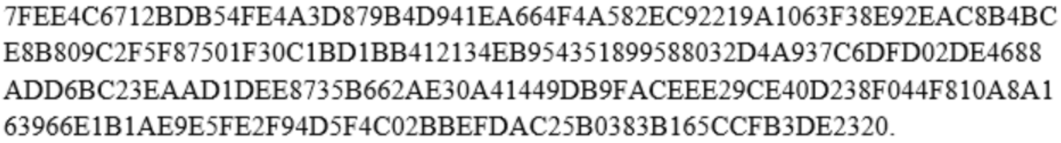


Figure 8. The m-sequence generated by a linear feedback shift register with a generating polynomial of $x^{10}+x^6+x^5+x^3+x^2+x+1$.

After adding a 0 at the end to balance the number of 0 and 1 bits, we have a sequence of 1024 bits as follows:

1111111110111001001100011001110001001010111101101101010100111111
1001001010001111011000011110011011010011011001010000011110101001100
0110010011110100101001011000001011101100100100010000011001101000
0100000110001111110011100011101001001011101010110010001011010010111
1001110100010111000000001001110000101111010111111000011101010000001
1111001100001100000110111101000110111011010000010010000100110100111
0101110010101010000110101000110001001100101011000100000000001100101
1010100101010010011011111000110110111111101000000101101111001000110
1000100010101101110101101011110000100011111010101010110100011101111
0111010000111001101011011011001100010101011100011000010100100000010
1000100100111011011100111111010110011101110111000101001110011100100
0000110100100011100011110000001000100111111000000010000101010001010000
0101100011100101100110111000011011000110101110100111100101111111100
0101111100101001101010111110100110000000010101110111110111111011010
1100001001011011000000111000000111011000101100101110011001111011001
111011111000100011001000000.

Converting to hexadecimal system we have:



7FEE4C6712BDB54FE4A3D879B4D941EA664F4A582EC92219A1063F38E92EAC8B4BC
E8B809C2F5F87501F30C1BD1BB412134EB954351899588032D4A937C6DFD02DE4688
ADD6BC23EAAD1DEE8735B662AE30A41449DB9FACEEE29CE40D238F044F810A8A1
63966E1B1AE9E5FE2F94D5F4C02BBEFDAC25B0383B165CCFB3DE2320.

The Linear Feedback Shift Register corresponding to the generating polynomial $x^{12}+x^{11}+x^{10}+x^{8}+x^{7}+x^{2}+1$ will generate 4095 pseudo-random sequences m.

Figure 9 depicts the result of an m-sequence generated by a linear feedback shift register with a generating polynomial of $x^{15}+x^{14}+1$. The Linear Feedback Shift Register corresponding to the generating polynomial $x^{15}+x^{14}+1$ will generate 32767 pseudo-random sequences m.

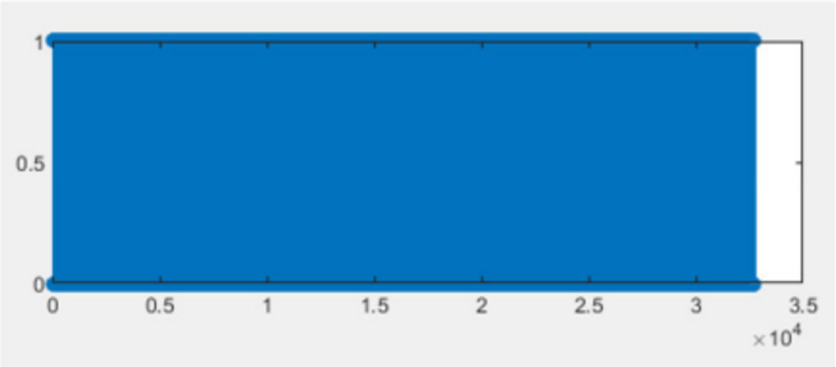


Figure 9. The result of an m-sequence generated by a linear feedback shift register with a generating polynomial of $x^{15}+x^{14}+1$.

Conclusion

The content of this paper is to research on finite field theory and D transform, non-orthogonal multiple access, Interleave Division Multiple Access, IDMA Transmitter, IDMA Receiver, Generate a pseudo-random signal for interleaver. The article proposes a Gold code generated from two pseudo-random strings m to generate the code for the interleaver. Gold chain generator diagram example, which combines two m sequences the m corresponding to generating polynomials $x^6+x^5+x^2+x+1$ and $x^6+x^5+x^3+x^2+1$. The Gold sequence generator from two m sequences of degree 6 was proposed and simulated, resulting in 65 pseudo-random codes. The Linear Feedback Shift Register corresponding to the generating polynomial $x^{10}+x^6+x^5+x^3+x^2+x+1$ will generate 1023 pseudo-random sequences m. The Linear Feedback Shift Register corresponding to the generating polynomial $x^{12}+x^{11}+x^{10}+x^8+x^7+x^2+1$ will generate 4095 pseudo-random sequences m. The Linear Feedback Shift Register corresponding to the generating polynomial $x^{15}+x^{14}+1$ will generate 32767 pseudo-random sequences m. When the actual 5G mobile communication network needs to increase the number of random pseudocodes, we can use a Linear Feedback Shift Register with a higher order generation polynomial. Choosing a generating polynomial with degree m large enough will create more bit sequences and increase the number of bits per code. Depending on the actual number of users on the 5G system, we will optimally choose m. Corresponding to a polynomial of sequence m where N = $2^m - 1$ incomplete sequence '0' is defined, that is, the set of N different phases (roundshifts shifts) of y = {yn} is called: y, Ky, K2y ..., K(N-1)y. In which, Km is a symbol that allows to shift a vector to the left m positions. If y = {y_n} = (y0, y1, y2,…, yN-1) then Ky = (y1, y2, y3,…, yN-1, y0), K^2y = (y2, y3,…, yN-2, yN-1, y0, y1), …, K^Sy = (yS, yS+1,…,yN-1, y0,…, yS-1).

Reference

[1]. D. Hao and P.A. Hoeher, *"Iterative Estimation and Cancellation of Clipping Noise for Multi-Layer IDMA Systems,"* in Proc. 7th Int. ITG Conf. on Sour. and Chan. Cod. (SCC), Ulm, Germany, pp. 1–6, Jan. 2008.

[2]. Dr. S. Syed Ameer Abbas, *"Realization of NOMA Scheme using Interleaved Division Multiple Access for 5G*", International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number 12 (2018) pp. 10580-10587.

[3]. L. Ping, *"Interleave-division multiple access and chip-by-chip iterative multi-user detection,"* IEEE Commun. Mag., vol. 43, no. 6, pp. S19–S23, Jun. 2005.

[4]. P.A. Hoeher and X. Wen, *"Multi-Layer Interleave Division Multiple Access for 3GPP Long Term Evolution,"* in Proc. IEEE Int. Conf. on Commun. (ICC), Glassgow, Scotland, pp. 5508–5513, Jun. 2007.

[5]. P.Z. Fan and M. Darnell (1996), *Sequence Design for Communications Applications*, New York: Wiley.

[6]. R.G Gitlin & J F Hayer, *"Timming recovery and scramblers in data transmission"*, Bell Syst Tech Journal, vol 54, no3, pp 589-593, March 1975.

[7]. Ruhir Gupta, Manoj Shukla *"Performance Analysis of Optimum Interleaver based on Prime Numbers for Multiuser Interative IDMA Systems"*, Article in International Journal of Interdisciplinary Telecommunication and Networking, August 2010.

[8]. T.T.T. Nguyen, L. Lanante, Y. Nagao, and H. Ochi, *"Low Complexity Higher Order QAM Modulation for IDMA system,"* in Proc. IEEE Wireless Commun. and Net. Conf. Work. (WCNCW), New Orleans, USA, pp. 129–134, Mar. 2015

[9]. Tran Canh Duong et al (2021). *Generating the interleave division multiple access (IDMA) used in 5G mobile communication system*. Journal of Xidian University - ISSN No:1001-2400- Volume-15-Issue-12-December-2021 pp. 546-534.

[10]. Truong Dang Van, Hieu Le Minh, Binh Nguyen Thanh, Quynh Le Chi - *Construction of Nonlinear Ternary m-sequences with Interleaved Structure by d-Transform.*

[11]. X.D.Lin and K.H.Chang: *"Optimal PN sequences design for quasisynchronous CDMA commu- nication systems"*, IEEE Trans. Comm.vol 45. pp 221-226. Feb 1997.