GENERATING PSEUDORANDOM CODES

PhD Student **Ion POPA**

Tehnical University "Gheorghe Asachi" of Iasi
Faculty of Electronics, Telecommunication and Information Tehnology

REZUMAT. În această lucrare este prezentată o modalitate de generare a codurilor de împrăştiere utilizand programe realizate în Matlab. Pentru studiu am luant în considerare trei tipuri de secvenţe de cod : secvenţă M ,secvenţă Gold şi secvenţa Gold ortogonal ,iar pentru fiecare secvenţă de cod am realizat câte un program în Matlab. Aceste programe sunt notate în lucrare astfel: *„create_ sequence_ M "and „ create_ sequence_ gold „*. Pentru validarea acestor secvenţe am realizat două programe : "*autocorrelation_ type_ M*" „şi „*correlation_ type_ M* „. Cu ajutorul programului „*autocorrelation_ type_ M*" se poate calcula funcţia de autocorelaţie pentru fiecare secvenţă de cod iar cu programul „*correlation_ type_ M* " putem verifica dacă două secvenţe de cod îndeplinesc condiţiile de „pereche preferată". Aceste programe sunt necesare atunci cand dorim sa ralizam studii de performanţă pentru sisteme de comunicaţii mobile care folosesc tehnologia CDMA

Cuvinte cheie: funcţia de autocorelaţie , funcţia de corelaţie , secvenţă M, secvenţă Gold şi secvenţă Gold ortogonal

ABSTRACT : This paper presents a method of generating pseudorandom codes, using programs made in Matlab. For this study, we considered three types of code sequences: M sequence, Gold sequence and orthogonal Gold sequence and for each code sequence we realized one program of generating in Matlab. This programs are noted: "*create_ sequence_M*" and „*create_sequence_gold*". For validation of these sequences we realized two programs: " *autocorrelation_ type_ M* " and " *correlation_ type_ M* ". Using the "*autocorrelation_ type_ M*" program it can be calculated the autocorrelation function for each code sequence which was generated and using the "*correlation_ type_ M* " we can calculate the correlation of code sequence and we can verify which of the code sequence satisfy the "preferred pair"conditions. This programs are very important when we want to realize performance study for mobile communication system, which uses the CDMA technology.

Keywords: autocorrelation function, cross-correlation function, M sequence, Gold sequence, orthogonal Gold sequence.

1. INTRODUCTION

For mobile communication systems that uses multiple access CDMA technology (Code Division Multiple Access), the choice of code sequence type is important for the resistance against interference with other domeins and against interference with a high number of users. Sequences should be as different as posible but at the same time to be easily reproduced at the reception. The most simple code sequences, are the random ones where each chip is selected randomly between values 1 and -1. These sequences are known as pseudo-noise sequence (pseudo-random). To be used as direct-sequence, pseudorandom sequence must carry out the following conditions.

- Sequences must be composed from numbers with two levels.

- Autocorrelation function must have a maximum, on the length of a chip.

- Sequences must have a low value of correlation.

- Code sequences must be "balanced" (the difference between 1 and 0 in the code can be only 1).

2. CODE GENERATION BY LINEAR FEEDBACK SHIFT REGISTERS

There are several ways to generate code sequences. One is by the use of feedback shift registers and this method is the one generally used in CDMA systems. A shift register contains a number of cells (numbered 1 to n), and each cell is a storage unit that under the control of a clock pulse, moves its contents to its output while reading its new contents from its input. In the standard configuration of a feedback shift register the input of cell m will be a function of the output of cell m-1, and

output of cell n (the last cell of the shift register) form the desired code sequence. Fig.1 shows a serial shift register with feedback.

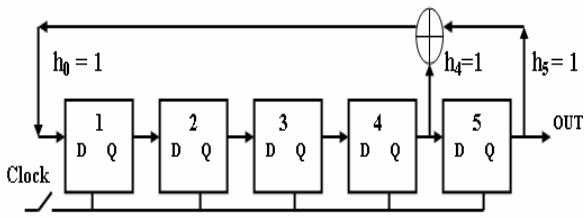

Figure 1 Serial shift register with feedback

Fig.1 shows a serial shift register with linear feedback function, which can generate a sequence from generator polynomial h (x) = $x^5 + x^4 + 1$. In general the configuration of a shift register with feedback is described by a generator polynomial which is a binary polynomial of degree n. The number n is the number of sections of the shift register. Generator polynomial is given by (1).

$$h(x) = h_n x^n + h_{n-1} x^{n-1} + \cdots h_1 x^1 + 1 \quad (1)$$

In Fig.1, n = 5 and polynomial generator is h (x) = $x^5 + x^4 + 1$ where $h_0 = h_4 = h_5 = 1$.Using this shift register, we can generate many code sequences for spread spectrum signal. Below is presented a way to generate three types of code sequences using programs made in Matlab.These sequences are: M sequences, Gold sequences and orthogonal Gold sequences.

3. GENERATING M SEQUENCES

M sequences are generated by a single serial shift register. Length and maximum number of sequences that can be generated with this circuit are given by the relation:

$$N = 2^n - 1 \quad (2)$$

where n is the number of cells in the serial shift register. To generate a sequence M, the generation polynomial must be a polynomial of degree n. Thus, autocorrelation function of a sequence M is given by:

$$r_{xx}(t) = \frac{1}{T} O_0^T x(t)x(t+\tau)d\tau \quad (3)$$

with the following values:

$$\begin{cases} 1 & \text{for } t = 0, N, 2N. . \\ -\frac{1}{N} & \text{otherwise} \end{cases} \quad (4)$$

A so-called "preferred pair" is a combination of two M sequences for which cross-correlation function has only three different values { -1,-t (n), t (n) -2}. Gold and Kasami have shown that there are pairs of M sequences of length n, which have three values for the cross-correlation function { -1,-t (n), t (n) -2 } where:

$$t(n) = \begin{cases} 1 + 2^{(n+1)/2} & \text{for } n = \text{odd} \\ 1 + 2^{(n+2)/2} & \text{for } n = \text{even} \end{cases} \quad (5)$$

To generate M sequences, we use the program called: "*create_sequence_M (nr_cell, feedback, init n_secv)*". The arguments of this function are: the number of cells "*nr_cell*" position of the reaction function "*feedback*" initial values of registers "*init*" and the number of outputs "*n_secv*". For example, suppose that the number of registers is 3, initial values of registers are [1, 1, 1], with, the reaction function between registers 2 and 3. Generator polynomial is given by equation (6).

$$h(x) = x^3 + x^2 + 1 \quad (6)$$

The shift register configuration for generating a M sequence is shown in Fig.2

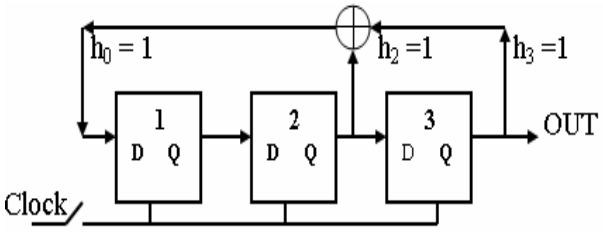

Fig. 2 .A shift register with three cells

To generate a sequence M in Matlab using the following command:

>> m1 = create_ sequence _M (3, [2, 3], [1 1 1]). In this case we considered a shift register with 3-cell, feedback function between registers 2 and 3, initial values of registers are [1 1 1]. Generated sequence is:

m1 = 1 1 1 0 0 1 0

We obtain a M sequence, with the vector length equal to 7 (length = 2^n-1 where n = number of cells). When the number of outputs *n_secv* is given, the number of sequences generated is equal to *n_secv*. For example, another M sequence is generated by the following command:

>> m2 = create_ sequence_ M (3, [2, 3], [1, 1, 1], 2)
When we use this command we obtain sequence:

ans =

1 1 1 0 0 1 0

0 1 1 1 0 0 1

If the reaction function is between the first and third register, the code sequence can be generated with the following command:

>> m3 = create_ sequence_ M (3, [1, 3], [1, 1, 1])

We obtain: m3 = 1 1 1 0 1 0 0.

Using programes: "*autocorrelation_ type_ M*" and "*correlation_type_ M*" we can evaluate the characteristics of M sequences. Because the generated code sequences consist of 0 and 1, the code sequences are converted into code sequences consisting of -1 and 1 by the folowing command:

*>> m1 = m1*2-1;*

*>> m3 = m3*2-1;*

The autocorrelation function of the M sequence is calculated using the following command:

>> autocorrelation _type _M (m1)

ans =7 -1 -1 -1 -1 -1 -1

>> *autocorelation_type_M (m3)*

ans =7 -1 -1 -1 -1 -1 -1

From calculation of cross-correlation function between m1 and m3 we use the following command:

>> correlation_ type_ M (m1, m3).

We obtain:

ans =3 3 -5 -1 -1 3 -1

From the above results we see that for m1 and m3 autocorrelation function satisfies the relation (4) and cross-correlation function has only three values (-1, 3 and 5) respectively (-1, -t (n) and t (n) -2) where t (n) = 5 for n = 3 (n = number cells of shift register). In these conditions, we can say that m1 and m3 sequences are "preferred pair" so that sequences can be used for the spreading code. If we consider two sequences some: m4 = [-1, -1, -1, -1, 1, 1, 1] and m5 = [-1, -1, -1, 1, 1, 1,-1] for which we calculate the autocorrelation function and cross-correlation function we obtain:

>> *autocorelaion_type_M (m4)*

ans = 7 3 -1 -5 -5 -1 3

>> *autocorelation_type_M (m5)*

ans =7 3 -1 -5 -5 -1 3

Calculating cross-correlation function for m4 and m5 we obtain:

>> correlation_ type_ M (m4, m5).

ans =3 -1 -5 -5 -1 3 7

These results show clearly that the two sequences m4 and m5 are not valid M sequences because the value of autocorrelation function do not satisfy relation (4) and values of cross-correlation function are different from the values: [-1,-t (n), t (n) -2] where t (n) = 5.So sequences, m4 and m5 may not have the characteristics of a “preferred pair "and therefore these two sequences can not be used for spreading the signal. Usually, M sequence has good features for the autocorrelation function, however, the number of mobile communication systems, which use M sequence is very low.

The number of M sequences, which have the same length and same features of the autocorrelation function is limited. When we make a CDMA system where multiple users communicate with each other, it needs several sequences with different codes and which have

the same value of correlation. Gold sequence is such a sequence.

4. GENERATING GOLD SEQUENCES

The Gold sequence is generated by exclusive OR (EXOR) of two M sequences, whose relationship is that of a"preferred pair".The generation circuit is shown in Fig 3.

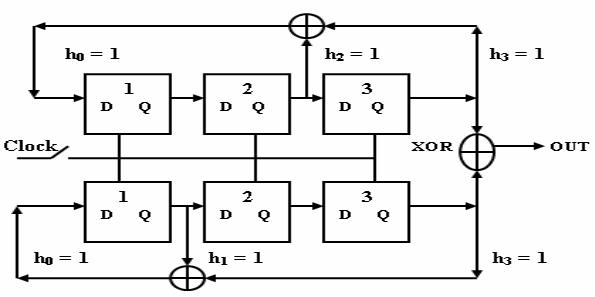

Fig.3.The circuit for generating Gold sequences.

For Gold sequence generated from two M sequences, the cross- correlation has three values {-1,-t (n), t (n) - 2}.To generate of Gold sequences, use the program, "*Create Gold Sequence*" developed in Matlab, where the function of generating Gold sequences is marked "*create_sequence_ gold(x1, x2, n_secv)"*.The arguments of this function are sequences x1, x2 and the number of outputs, denoted "*n_secv*". To generate Gold sequence we need, two M sequences , which should be, " preferred pair ".To generate Gold sequence, we must perform the following steps:

First we generate the m1 and m2 sequences. Then we check if the sequences are "preferred pair. If, the sequences are "preferred pair" we will generate Gold sequence.

>>m1 = create_secvence_M(3, [1, 3], [1, 1, 1])

ans = 1 1 1 0 1 0 0

>> m2 = create_secvence_M(3, [2, 3], [1, 1, 1])

ans = 1 1 1 0 0 1 0

m1 =m1*2-1

m1 =1 1 1 -1 1 -1 -1

>> autocorelation_type_M(m1)

ans = 7 -1 -1 -1 -1 -1 -1

>> m2 =m2*2-1

m2 = 1 1 1 -1 -1 1 -1

>> autocorelation_type_M(m2)

ans =7 -1 -1 -1 -1 -1 -1

>> corelation_type_M(m1,m2)

ans = 3 -1 3 -1 -1 -5 3

>> g1 = create_secvence_gold (m1, m2)

g1 = 0 0 0 0 1 1 0

From the above results is noticed that the m1 and m2 sequences are "preferred pair" and therefore can be used to generate a sequence Gold. To generate Gold sequence, we use the command:

>> g1 = create_secvence_gold (m1, m2)

Therefore, we obtain a Gold sequence in three stages [0 0 0 0 1 1 0] with a length of vector equal 7.Changing the initial values of shift register "*init*" we can obtain a different Gold sequence. If the number of outputs "*n_secv*" is given, we can obtain N Gold sequences. For example, when we use the following command:

>> g1 = create_secvence_gold (m1, m2,2)

ans =

0 0 0 0 1 1 0

1 0 0 1 1 0 1

Using functions "*autocorrelation_type_M*" and"*correlation_type_M*", we can evaluated the characteristics of Gold sequences.

>>g1 =g1*2-1

g1 = -1 -1 -1 -1 1 1 -1

>> autocorelation_type_M(g1).

ans = 7 3 -1 -1 -1 -1 3

In this case the autocorelation function has the following values:[7, 3, -1, -1, -1, 3]. The autocorrelation has high value in the synchronization point but in other points, the data fluctuates. To calculate the cross correlation value another Gold sequence must be generated, for which we follow the same steps as above.

>> *m3= create_secvence_M (3, [1, 3], [1, 0, 0]);*

m3 = 0 0 1 1 1 0 1

>> *m4 = create_secvence_M (3, [2, 3], [1, 0, 1]);*

m4 = 1 0 1 1 1 0 0

>> *g2= create_secvence_gold (m3, m4)*

ans =1 0 0 0 0 0 1

Cross-correlation value of g1 and g2 is obtained using the following command:

>> *corelation_type_M(g1,g2)*

ans = -1, 3, -1, -5, -1, 3, -1

We obtain the value [-1, 3, -1, -5, -1, 3, -1]. This result has three values {-1,-t (n), t (n) -2}, where t (n) = 5. Gold sequence has many different codes compared with the M sequence. However, there are some problems associated with Gold sequence:

-Ratio of 0-1 is not always balanced.

-The cross-correlation of Gold sequence is not 0, in a synchronize modium.

-To generate Gold sequences it needs a special synchronization.

To solve the problems mentioned above, it is added a chip Gold sequence to balance the 0-1 proportion. This sequence is called orthogonal Gold sequence. Cross-correlation value, of orthogonal Gold sequence is 0 at the point of synchronization.

5. CONCLUSIONS

Based on the results which were presented in this paper, we can conclusion that using the programs: *„create_sequence_M”,”autocorrelation_type_M” „correlation_type_M”, „create_ sequences_ gold”*, we can generate the following pseudorandom sequences, which can be used for spreading the signals: M sequence, Gold sequence and orthogonal Gold sequence. Using this programs we can identify the code sequences which have the characteristics of a „preferred pair” too. This possibility of verification the generated sequences is very important for the selection process of code sequences which follows to be used at signals spreading.Changing the“*feedback*” and “*init*”arguments for the ”*create_M_sequence*” function, we can generate code sequences with different structures(the position of values from 1 to 0 will be different for each sequence) and changing the “*nr_cell*” and “*n_secv*” arguments also for this function , we can generate a different number of sequences with different lengths. Using this programs we can create our proper code sequences which we will use when we want to analyse the bit errors evolution for mobile communication system which uses the CDMA technology.

BIBLIOGRAPHY

[1] **Ion Bogdan** . *Managementul retelelor de comunicatii mobile* Ed. Politehnium Iasi 2008

[2] **V.P.Ipatov** *Spread Spectrum Signal and Systems &CDMA* 2001

[3] **Richard Schwarz**.*An Introduction to Linear Recursive Sequences J.Meel`s Pseudo Noise Secquences PN.*

[4] **Sampei, S.,** *Applications of Digital Wireless Technologies to Global WirelessCommunications*, Upper Saddle River, NJ:Prentice Hall, 1997.

[5] **Marin Ghinea**, *MATLAB Calcul numeric,grafica aplicatii.* Editura Teora 1997

[6] **Robert C. Dixon**, *Spread Spectrum Systems*, (John Wiley & Sons, Inc, 1984).

About the author

Eng. **Ion Popa,** PhD Student
„Gherghe Asachi „Technical University of Iasi
Faculty of Electronics, Telecommunication and Information Tehnology
email:ioanpopa57@yahoo.com